#03 SEPTEMBER 2018

PUBLISHED BY Secura

SecurAware

RECENT HACKS

Voting machine hacks and NetSpectre attack

INSIGHT

Artificial intelligence in healthcare

INSIGHT

The new WPA3 Wi-Fi standard

HACK

Targeted GPS spoofing

ADVICE

Security benchmarking in relation to international standards

PHILIP VAN GENDT, COMMERCIAL DIRECTOR AT SECURA SINCE JUNE 2018

The challenge is simply bigger and more interesting!

We are heading into the last quarter of 2018. So far, a year in which we learned again that the cyber threat is as expected, ever-increasing, evolving and a bigger topic than ever before. GDPR officially entered Europe on May 25th. Many organisations still struggle to really understand what is expected from them and how to get a grip. The information security industry in itself, can still be considered as 'struggling'. Many initiatives around standardisation and certification are emerging, but a Unified Information Security Assessment Framework on an international scale is still not in place.

For me personally, 2018 has been a year of change. 3 months ago I made a to many surprising but well-considered decision to move from a Sales Director position at Palo Alto Networks to become the Commercial Director at Secura. Many people did not understand my decision and asked me for my reasons to leave Palo Alto Networks, being world's #1 vendor for Next Generation Firewalls and Next Generation Security Platforms and still growing at unbelievable rates. My team was consistently successful. So, why walk away from this success story?

The challenge is simply bigger and more interesting! Protecting ourselves in the digital age goes way beyond protecting traditional infrastructures, cloud environments, endpoints and applications. The article "Targeted GPS spoofing" in this edition of the SecurAware describes a good example of such an evolution. In addition, a chain is as strong as its weakest link. It sounds dull and cliché, but it is true. Even when companies buy the best protection and prevention equipment on the planet, there is still the element of people and processes, being an inseparable component of information security. This is exactly what Secura witnesses on a daily basis. We assess the quality of information security holistically for society's most important organisations. Our ambition to play an even more important role in standardisation and certification is a huge contribution to keeping the digital world a safer place.

Secura has a great reputation. Since 2000, we top-rank the premier league for security testing, practicing vulnerability tests and pentests on the IT environments of the most renowned organisations. With the current management team's reputation in security standardisation and certification, Secura is expanding, enriching and improving its services. To conclude my motivation, I am very happy to have a product development team in place that helps to improve the level of our services by automating what can be automated, to allow customers to use our services on a continuous basis and to allocate the skills of our brilliant people in the most efficient way. Bottomline, we look forward to a very bright future.

After the re-branding in 2017 with the goal to transform from a pentesting company into a full-service organisation, we haven't been sitting on our hands. In several areas we booked a lot of progress;

We expanded our portfolio and divided it into 5 main categories:

1. Security Organisation
2. Security Testing
3. Security Certification
4. Awareness & Training
5. Tools

We introduced 3 tools:

- Secura Angler - a sophisticated phishing test platform aimed at both security awareness campaigns as well as offensive security assessments
- Secura purple box - a modular security test platform that enables executing a number of simulated attacks to probe an organisation's Blue Team, SIEM or SOC detection capabilities
- Secura ICCI – a tool to identify unexpected and unwanted network routes from within a secure network

Secura was recently officially recognized as a licensed laboratory to perform evaluations within the Baseline Security Product Assessment (BSPA) program of the National Communications Security Agency (NLNCSA).

Secura became a member of ECSO (the European Cyber Security Organisation) supporting the implementation of the Cybersecurity Act.

Enjoy this edition of the SecurAware and let us know how we can help you prepare for a secure 2019.

Warm regards,

Philip van Gendt,
Commercial Director

Remco Huisman has been the Commercial Director of Madison Gurkha & Secura from 2001 till recently. In March 2018 he decided to take a step back and continue as Senior Account Manager within Secura. Remco is still within Secura and partner of the company. Thanks for leading our sales team for many years Remco!

Secura licensed lab for BSPA

We are pleased to announce that Secura is officially recognized as a licensed laboratory to perform evaluations within the Baseline Security Product Assessment (BSPA) program of the National Communications Security Agency (NLNCSA). The recognition is granted on the successful completion of an extensive pilot evaluation project.

The announcement reconfirms the role and responsibility of Secura to test against defined security specifications in a limited timeframe and have the expertise necessary to evaluate the product in question. BSPA is another great example how a framework and further standardisation can help the industry to move forward and evaluate products in a defined, structured and consistent way.

We will tell you more about BSPA in an extensive article in the next SecurAware. For now, please refer to our website secura.com/press-release-secura-licensed-lab-for-bspa for more information.

Privacy from an informatics perspective

Matthijs Koot, senior security specialist at Secura, has written a chapter for the upcoming Handbook Privacy Studies, in a joint effort with professor Cees de Laat (University of Amsterdam). The book, edited by Bart van der Sloot and Aviva de Groot, will be published by Amsterdam University Press.

The handbook is a collection of perspectives on privacy by authors in various academic disciplines, such as law, ethics, politics, and economics. The chapter by Matthijs and Cees looks at privacy from an informatics perspective. During the Amsterdam Privacy Conference (5-8 October 2018), Matthijs will participate in a panel discussion about this. He also co-organized the conference track on privacy-enhancing technologies and encryption.

Amsterdam Privacy Conference 2018
5-8 October 2018
Amsterdam Roeterseiland Campus
https://www.apc2018.com

Symposium on Securing the IoT
29-31 October 2018
Crowne Plaza, Natick, MA
https://www.securingthenet.com

SecurAcademy
11 October 2018 Threat Modeling in vital infrastructure
25 and 26 October 2018 Mobile application hacking training
15 November 2018 Secure Programming course
29 November 2018 Hands-on hacking workshop Raspberry Pi
https://www.secura.com/securacademy

Securing the IoT

As hacking, phishing, DDOS and ransomware continue to increase, one thing is certain: securing the Internet of Things is critical to our survival! Razvan Venter, senior certification specialist at Secura speaks from experience and will present about Controlling Cybersecurity Risks in IoT by Standardisation during the symposium in the technology capital of Boston, upcoming October. He will give an overview on IoT standardisation state-of-the-art and highlight the way in which IoT manufacturers can benefit from it.

Join us and other speakers including Cisco, Silicon Labs, VDC for the Symposium on Securing the IoT. Early Bird Registration is now open! Please see the website for further details and registration: secura.com/symposium-securing-the-internet-of-things

Are you curious about our standardisation activities and vision on this topic? Please check our dedicated section on secura.com/security-certification or just contact us for more information.

COLOFON

Contributing editors
Christiaan Hillen
Erwin Janssen
Antal van Kolck
Ralph Moonen
Maayke van Remmen
Tom Tervoort
Razvan Venter

Art director
Hannie van den Bergh / Studio-HB

Contact
editorial@secura.com

Secura B.V.
Vestdijk 59
5611 CA Eindhoven
Netherlands

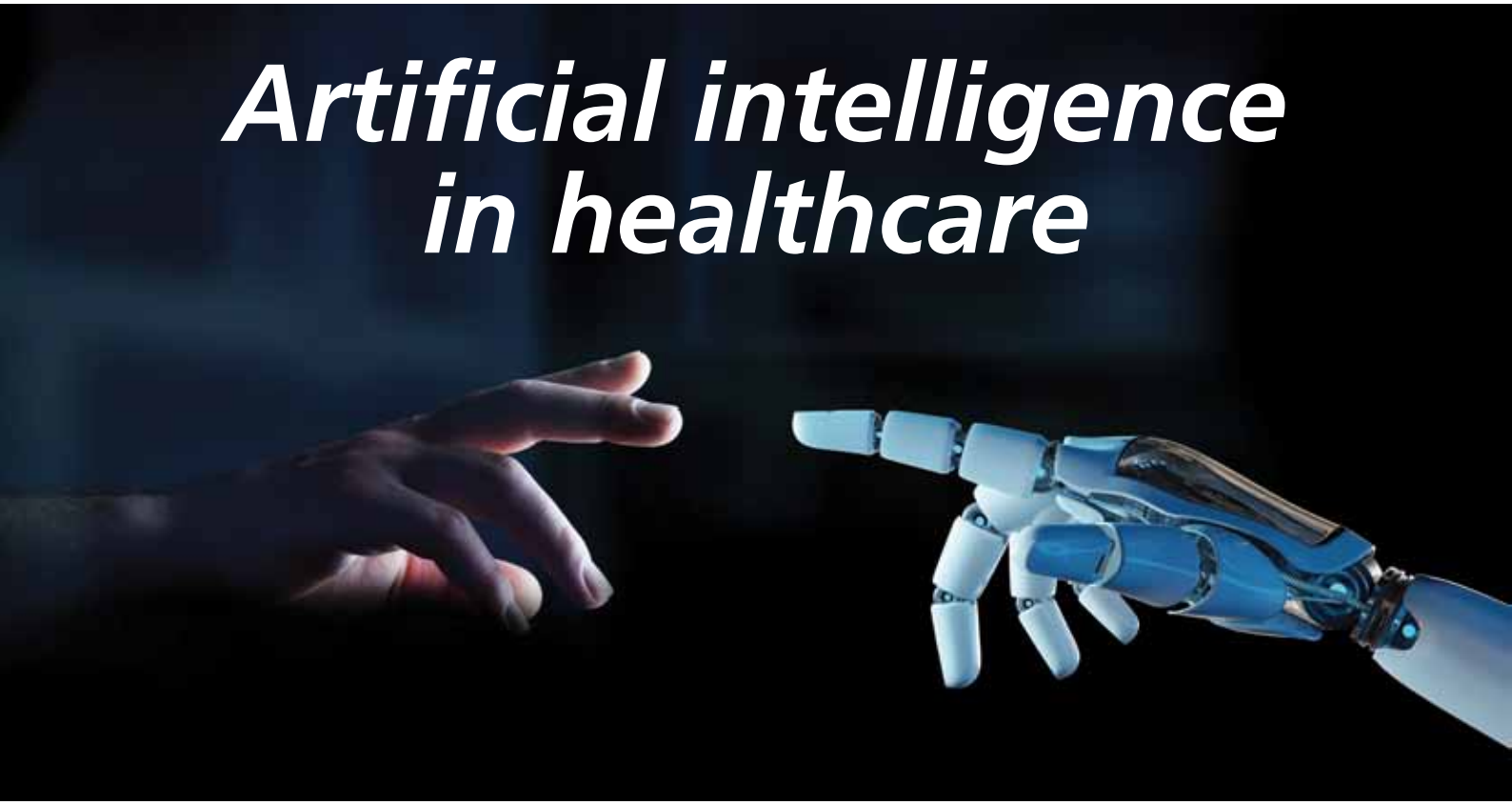
Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T + 31 (0)40 23 77 990
E sales@secura.com
W www.secura.com

Follow us on

Christiaan Hillen, Security Analyst

Artificial intelligence in healthcare



Artificial intelligence has an increasing effect on healthcare. As with any computer system, there are security risks involved. Christiaan holds degrees both in information science and healthcare, giving him an interesting cross-over perspective in these fields. AI in healthcare: how does it work and what aspects should you consider?

A year ago, a British artificial intelligence (AI) company called "DeepMind" was involved in a ruling concerning London's Royal Free hospital that failed to comply with the Data Protection Act. The hospital had provided personal data of around 1.6 million patients as part of a trial to test an alert, diagnosis and detection system for acute kidney injury.

This resulted in a nightmare scenario for anyone working with personal data, and in particular with data relating to healthcare. Not only the financial impact, but the loss of patient trust. The promises of AI in helping healthcare professionals to provide better care are clear but divides people in the healthcare business. You are either a critic, or you are an avid believer, up to such a level that it is more heretical to question the benefits of AI than it is to question global warming.

Machine learning

One of the core elements of AI is machine learning: given a large dataset, we want to know something; does someone belonging in group A (healthy) or group B (sick), that is, we want to classify the instances in the dataset, based on their attributes. For a computer to learn how to classify, it first needs to be trained to recognise and differentiate between people from group A and from group B. The process is straightforward:

- Get a large set of data containing people that are marked as belonging to group A or to group B.
- Split this set into smaller sets, each containing persons from group A and from group B.
- The computer gets one of these sets, with the markings A and B still attached.
- The computer learns how to classify these people; based on the attributes of each person. This step creates a model for the classification.
- After having learned this, the computer receives a random validation set, containing different people, to refine the model. Repeat as needed.
- The final set given to the computer is the (blind) test set, which is used to see if the model is able to correctly classify the subjects.

In simple cases, this process will result in a near 100% correctness of the model. In complex cases this might be difficult to achieve, something like 97% is more realistic. The computer might classify a person as sick while being healthy (false positive), or as healthy while being sick (false negative). Both can be detrimental to the patient. Even with a correctness of 97%, that leaves 48.000 of the 1.6 million that are incorrect.

Imagine an attacker going unnoticed, and being able to ever so slightly influence the model. Can he bring that 97% down to 94%, doubling the amount of incorrect classifications? Even a 1% change would have a significant impact. How do you know if your model has been altered? Security by design should be a part of any AI system.

Outliers

Models typically have problems with outliers. Data points that are very different from the usual, yet should fall within a certain classification. By definition, the number of outliers in a dataset is low. You might even not find one when training the model on the random set you generated. Such rare cases might be successfully identified by humans, but a computer that has never seen one, might not be able to combine all the attributes to come to the right conclusion.

Integrity checks on training data are important here, to be certain that outliers have not been removed or added.

Rare classes

In some datasets, there may be classes that are quite rare, yet closely related to a common class. Differentiating between these may be difficult, in particular if this small class is so rare that there are only a few instances in the dataset. If there are just one or two instances, the model will probably be able to identify them, but can fail in finding others. Say that all instances of this rare class in the model are male, the model might include a rule that to belong to this class, an instance then needs to be male. Females will be rejected outright. Models can be racist, sexist, and politically incorrect without scruples.

Correlation without causality

When training a model, correlations may show up that have nothing to do with the actual class of an instance. It may be through coincidence that the majority of patients with a patient number ending on a “5” belong to class A. As models have no (human) notion of what is and what is not important, these correlations may be used by the model to successfully classify subjects. Modern models are so complex that their inner workings and classification rules are nearly incomprehensible to humans. What takes a computer moment to understand, or days to create, can take years of human effort to fully grasp. Are you more susceptible to being “A” if your patient number ends with a “5”? Probably not, but the computer might think so. And how it got to that conclusion? Was it a programming error, a malicious insider, or a genuine result?

> “Are you more susceptible to being sick if your patient number ends with a ‘5’? Probably not, but the computer might think so.

> “If there are just one or two instances, the model will probably be able to identify them, but can fail in finding others

Test data

In order to properly train a model, more test data is always better. This may be why the data of 1.6 million patients was used by DeepMind. This test set is probably a very good representation of the overall population. Using such data for these purposes might actually be allowed under the GDPR, but do talk to your legal department about this before considering such an undertaking. An alternative is to create fictive data. This leads to a whole new set of problems however, which combines the already mentioned issues in training a model. How do you recreate outliers? How do you account for rare classes? Are you certain that all correlations (ignoring causality) are present in the set? If you randomise real data, you may lose key attributes that could improve classification. Creating fictive data altogether may not be representative of the population at all, in particular highly complex attribute-combinations.

Test data generation is a hard problem, and we don’t have a good solution for this. This is one of the reasons the GDPR allows for the use of personal data for scientific purposes, be it under strict conditions. It also mentions not using production data in a testing environment. Be sure to have regular checks with auditors to remain on the safe side.

Understanding

If you are using AI methods to gain insight in your customer data, be sure to know what you are doing. If you can’t explain to an independent auditor what it is exactly that you are doing with the data, and what decisions are being made based on the model that you created, you cannot harbor the expectation that your customers will understand either.

The security aspect

Do you have logs for all processing of the data? And are you certain that nobody takes home some of the data to work on their personal laptop in the evening? Who is responsible for the data? Who do you need to call when something goes wrong? How are the models validated, and are they securely stored where only authorised personnel can work with them?

Datasets for machine learning can be used to great, and devastating, effect. They can be used for good, and for evil. Protecting these sets and the models that are built with these sets, is therefore of paramount importance. Both the technical, and the organisational aspects of security need to be in order. Work together with auditors for this, they know what you should keep track of and how to comply with legislation whilst offering the best healthcare. Pentesters can help with identifying weaknesses in technical security. With great datasets come great responsibilities.

Razvan Venter, Senior Certification Specialist

Security benchmarking in relation to international standards

Investing most of the effort in functionality of the product and hoping for the best, or staying up to date with security measures and implementing them effectively? It's up to the organisations and manufacturers to make the right choice.

We are at a point where advances across industry are constant, and innovations in all technical domains are expected on a quarterly basis. Manufacturers and developers all over the world are investing billions in the hope of releasing the next big thing at the right moment. Under these circumstances, it is not hard to imagine that most of the attention is focused on the specs and functionality, leading to a superb user experience. After all, performance and design are what can be directly seen by the customers, and ultimately this is what creates the first impression of the product.

The importance of cybersecurity can be considered a paradox. Security cannot be seen by the common user (at least not directly) and yet, every once in a while, large scale attacks or vulnerabilities remind us about its importance, for example when IoT products are misused for these attacks. Besides this, there is the case of a nation's critical infrastructures such as transportation, banking, water, electricity, etc. As most of modern plants rely heavily on smart technology, disrupting their integrity or availability even for a matter of minutes could have a huge impact.

Importance of standardisation

Assuming (and hoping that) manufacturers and organisations decide to include cybersecurity in their main focus points, there is of course the question where to start and what is sufficient. Especially for small and medium-sized companies who cannot afford to invest into a dedicated security department, finding precise and up to date security specifications to guide them is of outmost importance. Here is where standards come into place. There are various standardisation bodies across the world of which ISO, IEC, ANSI, NIST and IEEE are the most well-known. The standards published by these bodies reflect the latest level of standardisation in various domains. For companies looking for a structural solution in the very complex domain of security, standards can provide the much-needed guidance and overall control.

Two important benefits of standards can be described as follows:

- They provide a confirmed view on a certain domain.
- They are recognized and acknowledged at national or international levels, thus providing professionals a common language for debate, comparison and alignment of objectives.

Standardisation is truly a holistic paradigm, as it can be successfully applied by manufacturers (of products or services) and organisations.

- By following a standardised way, manufacturers can make big steps in fighting the threats associated with their products or services, as well as showcasing the quality of their manufacturing processes and products. Various relevant standards could be in scope of manufacturers, depending also on the specific domain of applicability. IEC 62443 as well as UL2900 provide requirements for security features relevant for medical devices, industrial control systems or consumer IoT products. ISO 15408 (based on which the Common Criteria guidelines are built) provides a well-known framework for assessing I(o)T products. The Cloud Security Alliance Cloud Control Matrix is a state-of-the-art way of validating the security of cloud services, on which industry relies more and more heavily.
- Organisations can improve the security of their information systems by using standards such as ISO 27001, or dedicated frameworks from NIST, such as the NIST Cybersecurity Framework or NIST SP 800-53. More domain specific are the standards published by PCI (e.g. PCI DSS), which provide requirements for secure processing of payment transactions.

Developing standards is complex. However aligning them, successfully implementing them and validating the compliance to the standards is the challenge to focus on.

For companies looking for a structural solution, standards can provide the much-needed guidance and overall control

> Security benchmarking will enable you to showcase the security of your product, which could lead to a significant market advantage

Security benchmarking and certification

Besides including relevant standards into the development or process practices, a complementary activity is represented by security benchmarking. Benchmarking refers to the activity of having your security controls assessed and validated either internally in the organisation or by a 3rd party company. Such a validation could provide very useful outputs, such as:

- A confirmation that the used standards are correctly interpreted and applied in practice.
- A validation that the applied security controls are sufficiently effective to counter threats and risks.
- A confirmation that the used standards are up to date and the manufacturer or organisation is not unaware of any new applicable vulnerabilities.
- A consistent comparison with previous validations ensuring continues improvement and confirmation to the standard.

On top of benchmarking is the issue of certification. Certification refers to having your products or processes benchmarked by an accredited entity, usually called a laboratory, which is able to provide a recognised and independent opinion and issue an official certificate following the assessment. Such certificates are often used to prove the quality of implemented security controls and could provide a strong tool to obtain market advantage. Moreover, certification by an accredited third party could fight against fake security claims, therefore generally increasing the security level. Well-known examples of certification schemes for products and services are Common Criteria (for IT products), CSA Star Certification (for cloud service providers), or PCI PTS (payment devices). For organisations, the security of internal controls can be certified based on ISO 27001 (information security systems) or PCI DSS (bank account data processing). Finally, security professionals have multiple standards which they can use and even get certified in, depending on domain. ISO 27001 Lead Implementer/ Auditor, IEC 62443 Cybersecurity Expert or the CSA Cloud Security Professional are examples of personal certifications in line with well-known standards.

Towards a unified cybersecurity framework

By reading this article so far, one question could come to mind: with all the advantages of standardisation and certification, why is there no unified assessment framework on an international scale? The good news is that a general consensus does exist regarding the benefits of such an initiative. As a matter of fact, most of the cybersecurity conferences and events end with a debate on such a topic. Various initiatives are currently emerging, and the idea is discussed already for months at EU level institutions, which are busy with the publication of the EU Cybersecurity Act. The ultimate goal of this act is to come up with harmonised frameworks delivering “security seals” for certified products and services, similar in a way with the energy efficiency labels which can be found on all modern appliances or the CE marking on EU products. Secura is a member of security organisations related to this topic, actively driving the discussions and advancements. Examples of such organisations are ECSO (the European Cyber Security Organisation) and ENISA (the European Union Agency for Network and Information Security), both supporting the implementation of the Cybersecurity Act. Also on national level, Secura joined Cyberveilig Nederland which is an initiative of Dutch cyber security service providers with strong focus on aligning on risk model and a common certification framework.

While such initiatives are expected to take more time, we have good reasons to believe that cybersecurity benchmarking will soon find across industry the position which it deserves.

Ralph Moonen, Technical Director

Voting machine hacks

As usual, a number of interesting hacks and discoveries of vulnerabilities have taken place over the past few months. Often the impact and scope of such breaches and weaknesses only become clear after a while. In this case, we would like to take a closer look at voting machine hacks.

Elections in the Netherlands and other countries are supported by a number of digital tools. In some countries the voting itself is done on a machine, but not in the Netherlands. As you might know, this is a consequence of activist hackers who demonstrated that the machines were not capable of protecting themselves, and leaked information.

So we banned the voting machines in the Netherlands and reintroduced pencil and paper. But it turned out that that was not enough. When votes are tallied, they are sent to a central place, where the files are put on a computer and software is used to add up all the individual votes. As researcher Sijmen Ruwhof discovered[1], this process was also flawed to the extent that manipulation was easily possible, while being virtually undetectable.

Voting machine hacking at DefCon

Every year in August, voting machines are put to the test during DefCon in Las Vegas. DefCon is well-known for being the largest hacker conference in the world, and it is no surprise that there are enough people who love a challenge: hack the voting machines.

This year, just as other years, it turned out that voting machines have very serious and significant flaws. An associate professor from the Copenhagen University hacked one machine in just over an hour. Other examples include voting machines being hackable by simply plugging in a USB keyboard and hitting 'CTRL/ALT/DEL' after which access to the system could be achieved[2].

> Being able to remotely read memory is a very powerful attack

Even though we have seen the most important elections in the Netherlands last year, we have four elections coming up in 2019: Island Counsel Elections, Provincial State Elections, Watership Elections and the European Parliament. While the Dutch government is well aware of the shortcomings in the digital tooling that supports the election processes, acting on that knowledge is challenging. More security researchers will and need to take a good look at the voting processes in order to improve them and safeguard the integrity of our democratic process. The recent hacks at DefCon serve as a reminder that this has to be sorted out in between elections (i.e.: now) and not when armed with pencil and paper, ready to cast our ballot.

1. *https://sijmen.ruwhof.net/weblog/2053-security-assessment-of-dutch-election-software*
2. *https://www.cnet.com/news/defcon-hackers-find-its-very-easy-to-break-voting-machines/*

NetSpectre

Another important recent discovery this summer was the development of a variant of Spectre. This variant (called NetSpectre) does not require any malicious code to run on the target. Simply having network connectivity to the target can already be enough for an attack. How is this possible?

The Spectre vulnerability was/is exploitable, because differences in timing when reading memory were clearly measurable. With NetSpectre, things are a lot less clear. The timing effects are so small and smothered in noise, that only differential analysis and statistics can be used and even then, it takes 25 million measurements to discern 1 bit on a remote system in the cloud.

But honestly, 25 million measurements is nothing to an automated script. Let's assume that you are after a cryptographic key of 256 bits. Researchers were able to extract a byte every three hours this way. This means that the 32 bytes of that key can be retrieved in 96 hours, or four days. This is not a long time, if that key just happens to be a very important key!

Researchers will find new ways to optimize these types of side channel attacks and the four days will shrink further. Being able to remotely read memory is a very powerful attack. It hardly leaves a trace. While it can be detected, while it is being performed, it could also be hidden in legitimate traffic or slowed down in order to evade detection. SOC/SIEM implementations are not programmed to look for this attack yet, because it is pretty new and it remains to be seen how practical it really is.

We therefore do not foresee this method to be practically usable in penetration testing or red teaming projects for our customers in the near future. But intelligence agencies, state actors and sophisticated cyber criminals now have an extra weapon in their arsenal that has the power to break previously unbreakable things. It is a matter of time before this attack is spotted in the wild somewhere.

Cyberveilig Nederland: working towards a bright and safe future

As Secura, we strongly believe that focus on standardisation and national and international collaboration will give direction to improve cyber security. That is why we have become a member of a new industry platform: Cyberveilig Nederland.

Cyberveilig Nederland is a new industry platform of security service providers, who have the aim to increase digital resilience in the Netherlands and increase the quality and transparency within the growing cybersecurity sector.
In close collaboration with the government, Cyberveilig Nederland wants to give direction to improve cybersecurity within the Netherlands, by creating transparency within the industry trough development of a code of conduct and a security mark.

One of the focus areas of Cyberveilig Nederland is Quality and Transparency and they established a working group for this. Erwin Jansen from Secura is leading this. The Working Group Quality and Transparency is actively working on investigating existing cyber security standards and developing a vision and direction towards standardisation and certification. Multiple cybersecurity organisations are participating in this working group.

Moreover, Cyberveilig Nederland is one of the partners of the so-called "CCV-project" (Centre for Crime Prevention and Public Safety). This project aims for more expertise and trustworthiness of cybersecurity providers trough developing a risk model and a security mark. Cyberveilig Nederland is part of the steering committee of CCV in collaboration with the Association of Insurance companies, the Ministry of Economic Affairs, the Ministry of Justice and Security, Dutch Police and various branch organisations.

If you want to know more or want to discuss in more detail, please do not hesitate to contact us.

Erwin Jansen
Manager Service Line Security Certifications and Advisory & Audit
erwin.jansen@secura.com

Tom Tervoort, Security Specialist

The new WPA3 Wi-Fi standard

Recently, the Wi-Fi Alliance has released the improved Wi-Fi security standard WPA3, along with two sister standards. Will these improvements finally allow us to put more trust in the security of our wireless communications?

In the two decades since its introduction, Wi-Fi has become omnipresent: from laptops to TVs, from phones to 'smart' toothbrushes. And when devices want to communicate wirelessly (online or with each other) they are probably using Wi-Fi. Unfortunately the underlying protocols have had, until now, various vulnerabilities, that enabled attackers to eavesdrop wireless communication or gain access to restricted networks.

Being able to eavesdrop on, or modify data in transit is one issue, but it should not be forgotten that proper access control to networks can also be very important. This is usually not very problematic within typical home networks (although it may be annoying that the neighbors are using your bandwidth to stream Netflix or try to access your NAS). However it can become a significant issue in corporate settings, because for many companies, it can be beneficial to allow wireless access from employee devices to (parts of) the internal corporate network. An attacker who can subvert Wi-Fi security, may therefore be able to gain a foothold within the internal network, and use that as a basis for further attacks.

The state of Wi-Fi security today

A recent attack against WPA2, called KRACK, was published in October 2017, and allowed attackers to partially decrypt information from protected connections. In this case, vendors could apply patches that mitigate this issue without breaking compatibility. Unfortunately some issues with WPA2 are more fundamental in nature, and cannot simply be patched out without changing the protocol itself. Also, a new method for cracking WPA2 has been discovered based on retrieving the Pairwise Master Key Identifier (PMKID) from a router using WPA/WPA2 security, which can then be used to crack the wireless password of the router. Unlike previously known methods, no communication from other users needs to be eavesdropped. Furthermore, the cracking computation is sped up a few thousand times.

> It is currently very difficult to offer user-friendly Wi-Fi to people, without exposing them to significant risks

So, what are the Wi-Fi security issues that are still present today? Despite problems that can be mitigated by software patches or configuration changes, contemporary Wi-Fi standards still have the following problems:

- Open/public Wi-Fi is not encrypted and access points can be spoofed.
- WPA2 Personal passwords can be cracked offline.
- Users of the same WPA2 Personal network can decrypt each other's traffic.
- WPA2 Enterprise clients are difficult to configure securely.
- It is difficult to securely connect IoT devices.

Due to these issues, it is currently very difficult to offer user-friendly Wi-Fi to people, without exposing them to significant risks.

The new WPA3 standard

The new standards are supposed to address the vulnerabilities as discussed above. WPA3 once again defines two variations: WPA3 Personal (authentication with a password), and WPA3 Enterprise (authentication with user-specific credentials such as certificates). Furthermore, the Wi-Fi alliance has also released two related standards: Wi-Fi Enhanced Open (which is intended to improve security of public networks with no authentication) and Wi-Fi Easy Connect (a successor to WPS that offers an alternative method of connection).

Wi-Fi Enhanced Open

With the Wi-Fi Enhanced Open standard, it finally becomes possible to offer encrypted public Wi-Fi without requiring users to enter any password. Encryption in this case means opportunistic encryption: by performing a cryptographic key exchange, attackers

Protection against Wi-Fi attacks, per technology

	Open Wi-Fi	WPA2 Personal (PEAP)	WPA2 Enterprise	WPA3 Personal (PEAP)	WPA3 Enterprise	Enhanced Open	Easy Connect (QR code)
Passive sniffing	✗	✓	✓	✓	✓	✓	✓
Off-line password cracking	N/A	✗	✓	✓	✓	N/A	N/A
Active attack / spoofed AP	✗	✓	✓/✗[1]	✓	✓/✗[1]	✗	✓
Passive sniffing by an authenticated attacker[2]	✗	✗	✓	✓	✓	✓	✓
Active attack by an Authenticated attacker[2]	✗	✗	✓/✗[1]	✗	✓/✗[1]	✗	✓

1 Only protected when all clients are configured to verify certificates correctly
2 An attacker who has the credentials to access the network themselves, and targets other users of the same network

who passively sniff network traffic will not be able to find out what the key is, and can therefore not decrypt intercepted traffic. Unfortunately the scheme does not offer any mechanism to authenticate access points. This means that an active attacker who impersonates an access point can still trick clients into setting up an (encrypted) connection with them instead of the network they wish to connect to. They are still able to change and eavesdrop upon all traffic.

In practice, this means that open Wi-Fi is still insecure, it just means that attackers have somewhat fewer options for exploiting this fact.

WPA 3 Personal

WPA3 Personal offers the same type of functionality as its WPA2 equivalent: an encrypted Wi-Fi network to which you authenticate with a password. The most significant improvement of this protocol is the introduction of the SAE handshake protocol. SAE is a cryptographic password-authenticated key agreement protocol, which allows two parties (in this case a client device and an access point) to prove to each other that they are in possession of the same password, without revealing any information to a potential attacker that could be used to recompute this password.

Unfortunately, an attacker who already knows the password can impersonate the access point. This means that, even with WPA3, it is still not safe to publish the same password to multiple different users, because these users can then attack each other.

WPA3 Enterprise

WPA3 Enterprise disallows some deprecated authentication protocols, but only really offers one new option that is not already present in WPA2: namely 192-bit mode. While the gain from using 192-bit mode is limited (it doesn't address known cryptographic issues), perhaps some companies may find this mode useful for marketing or compliance purposes.

Wi-Fi Easy Connect

Wi-Fi Easy Connect attempts to address the problems WPS originally failed to solve: to make it more user-friendly to securely connect devices, even when these devices do not have a screen or method to enter passwords.

Unlike WPA3 or Wi-Fi Enhanced Open, this system can also be used to offer secure public Wi-Fi: put a QR code on a sign and any user who scans it gains access to a guest network. This is less of a hassle than having to type in a password, and can only be attacked when the attacker physically alters the contents of the sign.

Other key distribution methods are also defined: instead of QR codes it is also possible to use NFC or Bluetooth. Additionally, public keys can be transferred wirelessly, with the possibility to check their authenticity based on a shared secret.

Will WPA3 finally ensure secure Wi-Fi?

The new standards can be considered to be hit-and-miss: connecting to open Wi-Fi networks will remain dangerous despite implementation of Wi-Fi Enhanced Open. Major vulnerabilities in WPA2 are fixed, but some shortcomings are still present. The overview is present in the table.

The most promising of the standards is Wi-Fi Easy Connect, which among other things can be used to offer secure guest networks, or facilitate secure communication with and between IoT devices. When applied correctly, this has the potential of solving numerous security and usability issues at the same time.

Would you like to read more explanation and details after reading this article, please download the full white paper on our website: https://www.secura.com/whitepaper-will-wpa3-finally-ensure-secure-wifi

Maayke van Remmen, Marketeer

Black Hat Sessions

Thank you and save the date: 13 June 2019

Thank you to all participants, sponsors and partners for your contribution. We hope you all have enjoyed the conference. We look forward to organize next year's edition with even more in-depth presentations and hands-on activities. Hopefully you will be there (again)!


Adam Laurie


Ralph Moonen


Michel van Leeuwen

fotografie Martin Hols http://www.martinhols.com/black-hat-sessions-2018

On June 14th, 2018 the sixteenth edition of Secura's annual security conference Black Hat Sessions was organised. In this edition more than 300 participants were informed about the latest trends, threats and solutions in the world of digital security. Keynote speakers of this edition were: Adam Laurie (Director of ApertureLabs Ltd.), Ralph Moonen (Technical Director at Secura) and Michel van Leeuwen (Head of the Cybersecurity Policy Department, National Coordinator for Security and Counterterrorism, Ministry of Security and Justice in the Netherlands). Between the keynotes, we offered a large number of lectures given by prominent Dutch and international speakers in multiple technical and non-technical tracks.

Check out the aftermovie, photos, reports and all presentation recordings: secura.com/blackhatsessions2018

" Personal data processing is about trust, balance, ethics, culture and of course law. Therefore, privacy is not a one-dimensional challenge"

- Wolter Karssenberg

GDPR breakout session by:

- Wolter Karssenberg (Management Consultant Privacy)
- Ruud Kerssens (Secura)
- Fabian van den Broek (Radboud University)

"One user, one Excel file, one cell that contains a malicious command. That's enough to gain access to an entire organisation"

- Roy Duisters

Red Teaming breakout session by:

- Neal Conijn (SoSecure)
- Roy Duisters (Secura)

"At least 60% of smart buildings have systems that are extremely old, known as legacy systems, that lack basic protection mechanisms such as authentication or encryption" *- Elisa Costante*

IoT Security breakout session by:

- Elisa Costante (SecurityMatters)
- Nirvana Meratnia (University of Twente)

"More and more financial institutions use the Cloud but it is not regulated, according to the Dutch Central Bank "

- Miranda Chilvers

Certification breakout session by:

- Miranda Chilvers (Dutch Central Bank)
- Petr (BSPA team AIVD)
- Dirk Jan van den Heuvel (Secura)

This sixteenth edition of BHS featured a **Capture the Flag (CTF) competition** aimed at university student teams. There were sixteen challenges in four categories (Web, Crypto, System and Miscellaneous). The students had to, amongst others, break into the administrative interface of a website, reverse engineer binary code, do a forensic investigation and break the security of a blockchain implementation.

Congratulations to the winners

#1 EUR 2048 prize to team **THS** (University of Twente) #2 EUR 1024 prize won by team **HackerCat** (Delft University), #3 EUR 512 prize won by team **Factuur001.zip** (Delft University).

Luc Gommans & Bart Hermans, interns

Targeted GPS spoofing

Faking GPS signals (GPS spoofing) can make GPS receivers think they are somewhere they are not. This has been used to attack Navy ships[1] and is also possibly an effective way to perform dronejacking: forcing a drone to move, for example to guide it away from an airport.

The current technique, however, is not safe to use because it would impact all GPS receivers in a wide area. Therefore, Secura attempted to make GPS spoofing targeted: by splitting the GPS signal required for calculating a location over two directional signals, a target would experience the spoofing only at the intersection of the signals.

The GPS system uses a constellation of satellites. Each satellite basically transmits two things: where it is and what time it is. For example, a signal might be transmitted at 13:00:00.000 and arrive at 13:00:00.002: in those 2 milliseconds, the signal traveled 600km. You now know that you are 600km away from that satellite. By using multiple satellites, you can find the overlapping point in the equation and determine your position. This technique, determining a location using known distances to specific objects, is called trilateration.

Drones use GPS for flight assistance. If the drone software notices that it has moved to a position different from the pilot's instructions, then the change is probably caused by wind and will be corrected automatically. Also, if a drone loses connection to the controller, it will automatically trigger the 'return to home' function that is GPS-guided. Automated flights using waypoints are also an example of GPS-guided drone flight modes. By GPS spoofing, one can make the drone think it is slightly off its position or course, and force it to move in a certain direction, thereby controlling the actual position.

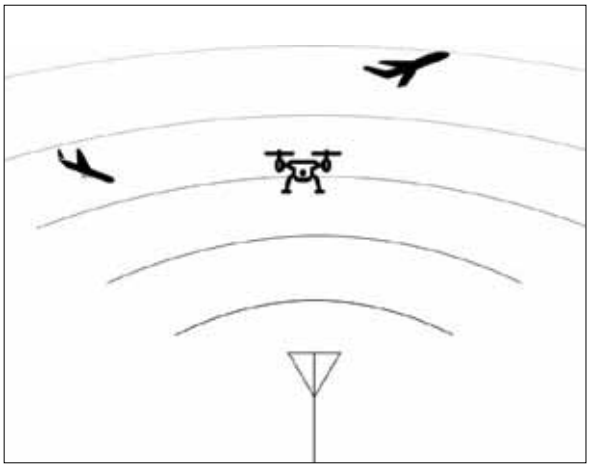
GPS spoofing software simulates what signals a receiver would receive at a certain position. It then modulates those signals and transmits them from a normal antenna. This means you don't need your own constellation of satellites to do GPS spoofing, equipment of a few hundred euros using a Software Defined Radio (SDR) is enough! The problem is that with current technology, one would disturb all other receivers in the area. It is therefore illegal to spoof or jam the GPS frequency.

This project is about making this spoofing attack specific to one receiver or a small area. The most interesting application of this is dronejacking. There have been several examples where an air ambulance (*traumahelicopter* in Dutch) could not land because a drone was in the way and the pilot of the drone could not be found in time. Geofencing[2] is not a viable solution, because a helicopter could land anywhere. Another example is a drone flying over a crowd: one cannot jam GPS and force it to land, because that might put people in the way of physical harm. Being able to reliably move the drone to a desired location would solve problems like these.

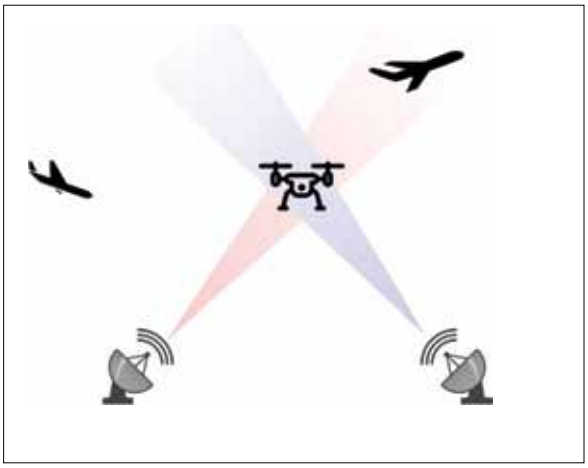
New approach

We wanted to combine the effect of two novel ideas: using directional antennas and splitting the signal over multiple antennas. There do not seem to be public reports on prior work on this.

Just using a directional antenna is not sufficient, as any other users in front of or behind the target will still experience effects of the spoofing. In practice, signals from at least four satellites are required for a position. By splitting the signals over multiple transmitters and transmitting the signals of only three satellites per each transmitter, only at the intersection of the signals, the target will see six "satellites", plenty to complete the location. Anywhere else, there are not enough satellites available.



Untargeted dronejacking



Targeted dronejacking

> We managed to build a proof of concept which does GPS spoofing using two directional antennas

In the set-up there were two Yagi-Uda antennas. When practically testing the antennas we confirmed that signals behind the antenna were weaker than in front of the antenna, but on the sides, the signal was barely reduced. Because of this, the idea could not be tested with the desired precision. In future work, it is recommend using another type of antenna, such as dish antennas.

For this project modified software, known as BladeGPS[3], was used to transmit the signals using two BladeRFs, with one antenna connected to each BladeRF. The main challenge here was time synchronisation: GPS requires nanosecond precision between transmitted satellite GPS signals. Very slight offsets already cause a large amount of error. In initial tests, the receiver calculated positions that were as far off as half a continent... and an altitude of literally 50% of the distance to the Moon! By using the system's high-resolution clock, the position error went down to 250 meters.

Conclusion

A proof of concept which does GPS spoofing using two directional antennas was succesful. While the error margin of the prototype version is still too high, it is clear that the technique works.

Due to the risks involved, testing on the real GPS frequency was not an option. In future work, tests should be conducted with better antennas and with the presence of the real signal. A more reliable implementation could clear the way for legislation to allow this technique to be used.

This project was conducted by Bart Hermans and Luc Gommans under the supervision of Ralph Moonen and Roy Duisters, as part of their master's thesis for the study Security and Network Engineering at the University of Amsterdam.[4]

1. https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

2. A geo-fence is a virtual perimeter for a real-world geographic area. A geo-fence could be dynamically generated—as in a radius around a point location, or a geo-fence can be a predefined set of boundaries (such as school zones or neighborhood boundaries).

3. https://github.com/osqzss/bladeGPS

4. For more details, please refer to this paper: Targeted GPS Spoofing. https://homepages.staff.os3.nl/~delaat/rp/2017-2018/p95/report.pdf

SecurAcademy

When it comes to training and awareness, Secura has as solid track record. Secura's experts are pleased to share their knowledge with you. The following practical training courses are planned and open to join.

Threat Modeling

11 October 2018

Learn how to use a threat modeling session to identify the threats that are applicable to the web application, mobile application, infrastructure or other component that is being threat modelled. We work on creating Data Flow Diagrams, identifying threats using STRIDE and mitigating identified threats.

Audience: This threat modeling course is specifically aimed at personnel of organisations that work in the vital infrastructure. Understanding of basic data flow diagrams and security concepts is required.

Secure Programming

15 November 2018

Train your developers to improve security at the creation stage. Learn how to find and exploit common vulnerabilities in web applications, such as Cross Site Scripting and SQL Injection, as well as steps to mitigate these issues when coding.

Audience: This course is intended for developers, who want to learn how to program more secure. Programming skills are required and a basic knowledge regarding the OWASP top 10 is needed.

Mobile Application Hacking

25/26 October 2018

Combining the fast world of security and mobile apps, this course teaches you how to assess mobile app security by our own Secura experts. Armed with in-depth information about the Android and iOS environment, your developers or pentesters will learn to identify security flaws in iOS & Android apps.

Audience: For this course technical background and expertise is required. Programming experience is not required, thought useful. Experience with the Linux command line is a plus.

Hands-on Hacking Raspberry Pi

29 November 2018

A fun and practical 1-day course to gain insight how hackers can break into your organisation. First, you will see how an attacker will become the Domain Administrator of an organisation after compromising the laptop of an employee. In the afternoon, in a practical session, you will setup a Raspberry Pi as an attack platform to gain this first foothold in an organisation.

Audience: For this course you need some basic technical/ programming skills as you will set up your own Raspberry Pi. Experience with the Linux command line is a plus.

All our training courses can be given in-house or, depending on the interest, open for public application.

secura.com/securacademy

TAKE CONTROL OF YOUR DIGITAL SECURITY