



Gion Sialm of the FOITT and Ivan Buetler of Compass Security share their experiences of web security with AdNovum CTO Tom Sprenger.

BROWSING THE WEB SAFELY

The security situation on the worldwide web is always in flux. Gion Sialm of the FOITT, Marc Condrau of Health Info Net and Ivan Buetler of Compass Security discuss the current developments with our CTO Tom Sprenger at the security round table.

Attacks are generally known as the greatest adversary to security. Which attacks do the most damage nowadays?

IB: Attacks by Trojans pose the main danger. Companies with large research departments and whose long-term success is dependent on the patents submitted have to deal with constant hackers' attempts to access their intellectual property. Espionage between states is done primarily using Trojan software as well. The second danger is posed by insider stories. Traditional phishing attacks on the web are declining, as they are often difficult and complex. Today, hackers make their way into the Content Management Systems (CMS) of publicly listed companies to obtain their quarterly results hours before they are published. If the hacker team has the know-how required to interpret the quarterly statements, they can do all kinds of highly speculative deals on the stock exchange.

MC: Phishing attacks and Trojans were and still are the most relevant dangers from HIN's point of view. We believe protecting the endpoint, typically the user PC, is crucial. User-friendliness is important here. Users will bypass security solutions with inadequate usability. Another central issue is making the user more aware.

What do today's users expect from an online portal in terms of security?

IB: To me personally, protecting the integrity of my data is important. When using free offers such as Facebook, Twitter etc., I know that I am giving away control and my data is the price. However, I can expect a business application not to pass on my data, to guarantee confidentiality and to stick to the existing regulatory requirements. The standards of the PCI (Pay-



(Marc Condrau's participation took written form.)

ment Card Industry) have to be adhered to when paying online with credit cards. Providers cannot save e.g. the CVC (three-digit code).

MC: Data protection is hugely important in the health sector. Maximum confidentiality and securely identifying communicators is absolutely necessary when accessing and exchanging data. On the other hand, the patient's comprehensive health data has to be available at all times. This balancing act often poses a challenge when designing security systems for the health sector.

Data is being used increasingly across organizations and business systems. How do you secure access within the company?

GS: The (Swiss) federation has clear regulations not just for access management, but also in terms of data protection. It is not permissible to use access data to draw conclusions about a person. If someone e.g. has access to VAT, he probably has his own company. That allows other conclusions to be drawn. That's why we need pronounced data separation. Each office sees only what it manages itself. We secure the data separation not only through regulations and processes but also in technical terms. That makes the solution more complex, but it is important for data protection.

IB: As a rule of thumb, I recommend controlling access near the data, if possible. Programming the web application profes-

sionally and safely is also crucial. However, implementation mistakes cannot be ruled out fully in practice. Thus, protecting web applications with an upstream web application firewall (WAF) to prevent such mistakes from triggering a serious accident or super-GAU is a wise strategy. That applies especially when you do not have any access to the web application's source code.

MC: Reliable authentication and authorization of the user is among the other prerequisites for safe, external access to internal data and functions. This is where HIN sets in as an Identity and Access Service Provider for the health sector. The use of validated HIN identities relieves application providers in inter-institutional data exchange. The HIN entry server infrastructure safely establishes the perimeter security of connected applications, e.g. for radiology systems in hospitals, and takes over the application authorization of external users.

PROTECTING WEB APPLICATIONS WITH AN UPSTREAM WEB APPLICATION FIREWALL IS A WISE STRATEGY. (IVAN BUETLER)

If you look at the developments in web applications architecture, a trend towards "app in a browser" stands out. GUIs are no longer sent back and forth in every call, but the whole application runs in the browser (e.g. HTML5). The communication with the backend is turning into technical data communication. How does this alter the demands on a WAF solution?

IB: The technical calls follow standards such as RESTful services, JSON or XML. The WAFs have to be able to understand and validate such protocols and technologies. Problems are occurring with "tunneled" protocols and protocols without open standards (such as ICA or GWT earlier) because the WAF cannot validate them. As long as the web permits proprietary formats for transmitting data, a WAF cannot offer any extensive protection on that level.

Are the new HTML5 applications an issue for the federation?

GS: Yes. We use HTML5 applications in combination with WAF and reverse proxy. We gain flexibility thereby and can intervene in various places for security reasons. Security is crucial to us and thus our supported security features must always be on the most up-to-date level. We are constantly developing our own security architecture and looking for ways to reuse parts of it and what has to be supported anew.



Let's return to data security. There are increasing encounters with application cases in which data leave the protected systems as they are given to third parties. Cloud services or collaborative services used among partners are just some of the examples. The classic perimeter security no longer applies here. Yet, we want to retain control of the data. What kind of approaches are there?

IB: Let's take e.g. e-banking which also presents "foreign" data in the shape of credit card bills. The ownership of the credit card bills does not lie with the banks, but with credit card companies. The e-banking gets a feed from the credit card producer and generates added value for e-banking customers. I see two security aspects here. Firstly, the provider's data (credit card data) can have damaging components. Thus, the bank should validate these data even if they come from a trustworthy partner. Otherwise there is the risk of a so-called second-order injection. Secondly, the credit card company reveals the ownership of the credit card data. What the bank actually does with that depends on the terms of the contract. The customer no longer knows where his data is.

Are there tools for circumventing the conflict of objective between data privacy and data exchange? In terms of government and e-health solutions, aggregated user data would add value. But to do so, people would have to accept their data leaving an organization's sphere of influence.

GS: An aggregation could certainly add value. This is done simply as such datasets need a legal foundation. Thus, if data is aggregated within an authority or across authorities, this is al-

ways based on an existing legal foundation. This means that data cannot be analyzed or aggregated without political consent.

**WE CAN ACHIEVE A HIGH LEVEL OF
SECURITY AND FLEXIBILITY
WITH HTML5 APPLICATIONS AND
A SECOND LINE OF DEFENSE.
(GION SIALM)**

MC: In the health sector, the aggregation of particularly sensitive health data with other data is a contentious issue. The federation's e-health strategy takes this into account by using its own patient identification for the patient's electronic file and not the AHV13 number.

Does that mean that companies and organizations have to consolidate their identities and means of authentication in time-consuming and expensive endeavors?

GS: Not necessarily. We have set up a federated architecture and managed to have PKIs, Kerberos, name/password, name/password/SMS and SuisseID authenticated in the federal administration in less than a year.

Do you believe it would be sensible to have an identity pool, which is managed centrally?

MC: Yes, we are fully convinced. HIN offers identities in the cloud as a service for the health sector. If institutions exchange data between each other, the application provider does not have to go to great effort identifying and registering the identities. The user gets access to over 50 applications via single sign-on. We have developed the HIN Access Gateway to facilitate a federated approach.

IB: I believe federated services have great potential in future. Companies will start making their users' identities available on the Internet via services such as Active Directory Federation Services (ADFS) so that cloud providers can profit from these identities. That saves time and money.

An interesting approach. Companies manage the identities and sign contracts with cloud providers. If a new identity is registered, it is automatically provisioned for the use of cloud providers.

IB: And vice-versa. If an employee leaves a company, his account is blocked on the company's own Active Directory and Federation Service. The block takes effect immediately and directly. The user cannot use either the company network or the federated services once his account has been blocked. Unfortuna-

tely, such federated systems are complex. The spread and use needs time to mature.

**FEDERATED SERVICES HAVE
GREAT POTENTIAL IN FUTURE.
(IVAN BUETLER)**

MC: Provisioning can also occur via the cloud in the internal IAM. This approach is interesting especially in the health sector where there is high staff mobility. Validated identity data, including information on medical and expert qualifications, can be taken over when a person joins an organization.

This is where the term “dynaxity” is apt – we increase both the dynamics by using federated services and the complexity by aiming for more services. That requires stricter governance...

GS: Definitely. Governance used to be faster than the technology. The monolithic architectures in particular were so complex that we spent years building them up. Today, governance lags behind technology. And the customers are hungry and make great demands. We need a good instinct for what is feasible without making things too complex.

Let's turn to authentication. That is currently an issue in the mobile sector in particular as demands on user-friendliness are generally high. What trends do you notice?

MC: Users of HIN services mainly use mTAN rather than card-based procedures on mobile gadgets. We are currently examining mobile ID.

IB: The authentication has to be above all simple. Complicated, certificate-based solutions such as SuisseID will not take hold across the range in my opinion. The opportunities for such systems lie in closed environments (e.g. the federation) or in applications with higher security needs (B2B or similar).

GS: E-government needs two things: A flexible IAM architecture and a good, simple means of authentication. We have PKI, but that device is as big as the mobile itself. What we like about SuisseID is that the management effort can be outsourced.

What could simple authentication look like?

IB: The user name/password authentication is successful because it's simple. It does not require software. You don't have to buy or install anything and anyone can do it. However, this kind of authentication is not very safe in my opinion. Analyzing

the conduct and properties of the client computer when authenticating can increase the security. A so-called “client correlator” examines the settings of the (user's) client computer, e.g. display resolution, installed plugins, browser language, average log-in time when authenticating and the provider's IP range. Such information reveals quickly who was at the computer before the user logs in with his password. In a project named “Panoptick”, the Electronic Frontier Foundation (EFF) has created a prototype, which demonstrates this technology.

MC: A simple user name/password authentication is not acceptable for external access in the health sector. To simplify the procedure for the provider of the application, the HIN platform offers different authentication procedures: certificate-based with Soft Token, mTAN, FMH's Health Professional Card and SuisseID.

Let's spin this thought further. Would solutions that do not require explicit logins be imaginable as long as you're not doing anything risky?



IB: An adaptive security system? That would be a good idea and very comfortable for the user. But in cases of e.g. a VAT repayment, there would have to be a step-up to a higher level of security. And the effort would have to be justified. If the user eventually has to install a client certificate for authentication, he could do that from the start.

If the client correlator gathers the attributes, the assessment is not as sharp. Can the risk be justified in your opinion?

MC: Access without explicit authentication is not imaginable for access to personal data in the health sector.

GS: The federation definitely needs a rethink. In certain cases, such as the VAT repayments mentioned above, such technology can only be used in combination with a procedure that rules out any blurs.

IB: Ultimately, it means that an analysis of data from the client computer can allow predictions about the user. Systems that use such techniques basically know before authentication who has been working at the other end of the line. Such profiling

**PROFILING IS IMAGINABLE
TO UNDERMINE ACCESS
IN THE EVENT OF UNUSUAL
USER BEHAVIOR.
(MARC CONDRAU)**

systems are already standard in the credit card industry. You pay a few centimes into a pool for damages with every credit card transaction. The credit card companies know precisely when and where a credit card is used. If a debt is incurred in South America while the owner is in Europe, that is automatically recognized and the owner goes unscathed. The credit card system thrives on the latent risk of abuse. This paradigm can be applied to other business cases.

Could the next security generation include profiling, if need be?

GS: As already mentioned, profiling needs a legal basis. Although Swiss citizens increasingly give their personal data to companies or social networks for profiling, it is very difficult to imagine this being allowed in an administration environment.

MC: Profiling in the health sector is imaginable, if access is undermined in the event of unusual user behavior, e.g. when health data is accessed from abroad. The usefulness is highly dependent on the specific application case.

IB: I see great future potential in profiling, i.e. in the compilation and use of users' profiles as well as applications, network traffic and similar. The correlation of data is central to research and security.

As we can see, the possibilities of using data on the web are by no means exhausted. At the same time, users are becoming more demanding and attackers more professional. Thus, protecting our data will remain on the agenda for the foreseeable future. Thank you for this fascinating talk. ■

Round table participants:

Gion Sialm

As head of IAM at the FOITT, Gion Sialm is responsible for access to federal applications. This central service at federation level functions almost exclusively as a trust broker. Internally and externally hosted applications are connected with the biggest authentication directories within and beyond the federation in a flexible manner. Access management remains under the control and responsibility of the commissioning departments themselves.

Marc Condrau

Marc Condrau is a solutions architect and project manager at Health Info Net AG (HIN). HIN was set up in 1996 on the initiative of the Swiss Medical Association (FMH) and the doctors' health insurance fund (Ärztelasse) with the aim of allowing Swiss health experts to use the Internet safely. HIN's core service is identity providing for care providers (approx. 17,000 presently). Secure e-mail services and access control services are offered based on HIN identities. Nearly all established care providers and over 420 institutions use HIN e-mail and over 50 application providers use the access control services.

Ivan Buetler

Ivan Buetler is the co-founder and CEO of Compass Security. Founded in 1999, the company has offices in Jona, Bern and Berlin and employs 35 people. It specializes in ethical hacking, penetration testing and security reviews. Ivan Buetler is an assistant lecturer at the University of Applied Sciences Rapperswil and at the University of Applied Sciences Lucerne. He organizes the European Cyber Security Challenge for Swiss Cyber Storm. He is the intellectual brain behind the Hacking Lab – an international laboratory for security professionals.