RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SPO3-R12

THE FASCINATION OF CONNECTIVITY—REDISCOVERED

Armin Graefe

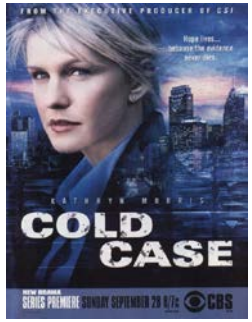
Security Evangelist, Head of Marketing
HOB GmbH & Co KG
www.hobsoft.com

Connectivity – a Cold Case

- Connectivity tools such as emulations or clients are widely perceived as **a class of products belonging to the past**.
- If their existence is noticed at all, they are **considered next to obsolete**.
- Some specimens of their kind, like SSH- or Remote Desktop-clients, **are tolerated**, but the underlying technologies would never be labelled “cutting edge.”

~~Connectivity~~ Cryptography – a Cold Case

- Advanced crypto-technology can be found in **the cheapest endpoint devices**.
- Most low-profile home devices can establish HTTPS connections.
  Juggling with huge prime numbers or using complex parameter sets for elliptic curves looks like **the easiest thing in the world** to the average user.
- The “consumer-type user” would **never** consider this an advanced technology.



About Slowliness

- Security professionals know that **cryptography moves in leaps and bounds** under its apparently quiet surface.
- Looking back only a few years, it becomes obvious that **algorithms rarely survive their inventors** and entire paradigms are given up in a matter of decades.
- Examples:
  - the “good old” RC4 stream cipher
  - the MD5 digest
  - the standard operations mode CBC

© Wikimeida

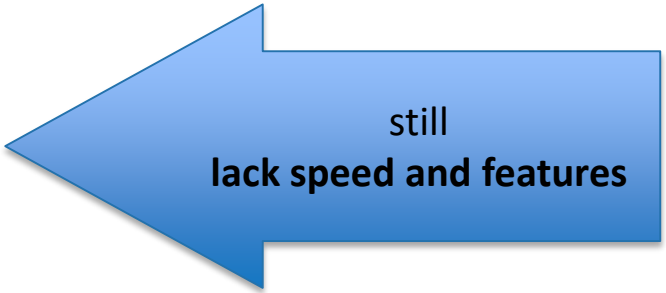
More About Slowliness

- It is even less known but equally true, that **connectivity also evolves at a remarkable speed**.
- Remote desktop access technology was extended multiple times, lately by protocol extensions for video streaming (UDP)
  and even some entirely **new concepts**
  like protocols that are based on
  video broadcast formats
  (to take advantage of hardware support).

© Wikimeida

Concerns in Connectivity

- Java is the basis of some successful remote desktop clients - it enables installation-free operation.
  Since Plug-Ins were banned from web browsers, **the acceptance of Java-clients has declined.**
- OS-specific clients excel in speed or peripheral device support; but they are **relatively hard to manage** in our multi-OS world.
- The new HTML5-based clients or emulations **seem to make all other approaches obsolete**.



What's so Boring About Security?

and Cryptography

- Cryptography is next to invisible and to the user John Doe, it looks way **too complex, boring or paranoid**.
- If John is below 30 years of age, he will probably fail see the point in using it, because **his life is perfectly documented** on the likes of Facebook® or Instagram® anyway.
- One big problem of today's cryptography is the fact that some powerful groups do not like it – and, in search of the weakest link, they usually try to **circumvent it.**

1

What's so Boring About Security?

and Cryptography

- **The biggest problem with security is negligence**.
- We should implement the privacy topic in **formal education**, from scratch. Certainly not a new requirement – but that does only make it more pressing.
- Generations of children use very powerful machines, which can easily destroy lives, **with very little serious and systematic safety advice.**

2

example: mobbing in social media

How can we expect someone that does not understand the mechanisms of a car crash to use a seat belt voluntarily?

IoT and Security – Discussed to Death

and still neglected

- Internet of Things is one of the rare cases that allows us to **retrace the development of our beloved worldwide web** in time lapse, like in a test tube.
- "**Functionality first**" and "full steam ahead" (or rather "never look back"?) seem to be the paradigms.
- Thousands of start-ups flood the market with ideas around the combination of everyday objects and Cloud technology.
- They just forget to implement **secure defaults** – or, at least, to provide adequate user guidance.

Take-Away

What happens out there

- Connectivity and cryptography are dirt-cheap and considered “a given.”
- Yet both, cryptography and connectivity, are steadily moving on.
- People fail to see the point in using them.

What you can do

- Make yourself aware of the steady improvements in cryptography **AND** connectivity.
- Foster the understanding of basic IT security and privacy concepts among your children – and no, 8 years is not too young.

HOW SECURE CONNECTIVITY WILL CONTRIBUTE TO USER SATISFACTION

The Future of Secure Connectivity

- Few would expect **disruptive technologies** to emerge in connectivity. In IT, this term is reserved for Cloud, IoT, AI or Big Data contexts.
- Yet simple tools such as Remote Desktop Clients introduce an **abstraction layer**, like a sandbox, that has some similarity to a web browser.
- From a security perspective, this is a **distinct advantage over tunnels**.
  Moreover, in contrast to browsers, this concept and its implementation are **rather simple** and jailbreaks hard to achieve.

The Future of Secure Connectivity

So the remote client of the future, what could it look like?

- It would have to provide a super-simple end-user interface.
- It would be **HTML5-based**, and all the functionality of “normal” clients would be included.
- It would support any kind of endpoint device and any kind of target.
- It would provide administrators real-time access to all connection metadata and integrate with SIEM and CASB systems automatically.

2

The Future of Secure Connectivity

HOB strives to push and extend the boundaries of connectivity technology. We are systematically developing new ideas.

Some nice features that you might find in upcoming versions of our products include:

3

- **Session roaming**
  Connections are transferred, instantly and seamlessly, between endpoint devices – cool stuff.
- **Flee-Latency connection broker**
  Users are redirected automatically to the network entry point with the lowest latency.
- **Push-Connections**
  Users stay in touch with co-workers without permanent checking of messages or mails because sessions are “sent” to them.

The Future of Secure Connectivity

4

- **RDP browsing**
  Internet browsing based RDP can help to protect both endpoint device and backend infrastructure from mutual infection. Ideally, the targets are “disposable” virtual instances.

- **Context-sensitive voice-controlled session launcher**
  The user asks the endpoint device for a connection, for instance to the CRM system to get the latest sales report, and the system spins up both session and application. Authentication could be voice- or picture-based.

Consumer Satisfaction is Key

If we look deeper into the latter suggestion, we catch a glimpse of the future issues in secure connectivity:

- We will soon live in a world where **every action is likely to trigger a connection**.
- Consumers are increasingly aware of the implications and, although industry may not be keen on having broad discussions about this topic, **people ask for more transparency**.
- They want to know where their devices transfer data and what kind of data it is. Even more: **the consumers ask for control**.

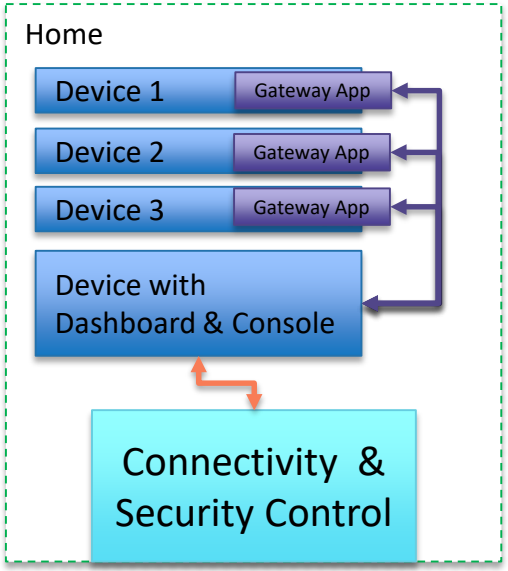
1

Consumer Satisfaction is Key

The IoT-market will drag a huge market for secure connectivity tools behind it to respond to the **consumers' demand for visibility and control**.

One promising concept is to combine connectivity and security tools in the sense of personal distributed gateways that **aggregate and analyze connection information**.

2



Take-Away

What happens in Connectivity

- Connectivity has some **surprisingly modern** security aspects.
- In the future, it will be more simple, fast, feature-rich and **truly client-less.**
- It will help users to **control their digital life**.

What you can do

- Check out the **advantages of simple connectivity tools** over complex technology such as tunnels
- Consumerization of IT leads to users that don’t understand the underlying concepts, but are **increasingly aware of the value of their data**.

ITSEC AND THE TRANSPARENT USERS

ITsec and the Transparent Users

- **Understanding connections and controlling them** – a group of people is focused on this aspect of connectivity:
  IT administrators and security staff.
- They enforce policies and analyze traffic using connectivity tools or the metadata that is provided by them.

  But here again, at the verge of the IT omnipresence era we are only getting started; **future generations of IT experts will dig much deeper** and go further than we imagine.

1

ITsec and the Transparent Users

As an example, we can look at a current hybrid cloud infrastructure.

- Firewalls or **UTM systems** - possibly combined with connectivity and/or remote computing platforms - **collaborate with SIEMs or CASBs.**
- Today's concepts make sure to identify devices, their users, and track activities, with a toolset that originates literally from a long-gone century:
  Old-school compliance checks, **crude** access restrictions, **all sorts** of reactive defense mechanisms.
- Even technologies considered elegant, such as behavioral heuristics, are not resolving problems in the long run, because they tend to add **complexity**.

2

ITsec and the Transparent Users

Tomorrow's engineers will have to go further.

- Some say, they will strive to understand the full history of any device that connects to their infrastructure.
- I doubt it, but they will certainly **trace the typical behavior of each user** in terms of times, places and activities and apply adaptive access controls in real-time, on a policy level, based on those individual usage patterns
- **Controls and analysis will be integrated and automated**; any abuse of a normally accessible function will lead to its deactivation within a matter of seconds.
- At the same time, the usage **metadata of individual connections will be aggregated and analyzed immediately** to detect patterns of systematic attacks.

3

ITsec and the Transparent Users

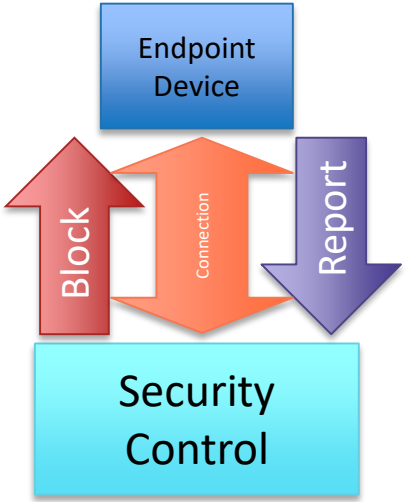
4

How does connectivity software fit into this picture?

Secure connectivity software can **interface with back-end security controls** to monitor activities and receive updated configurations in real-time.

It can go even further and constantly **check the client system and user interactions in real-time**, it extends the detection and defense capabilities to the front-end.

This approach makes log-analysis “after the fact” look clumsy and cumbersome.



Take-Away

What happens in Connectivity

- In the future, enterprises can improve **responsiveness** and overall security levels by combining security controls and connectivity tools, resulting in a **distributed, combined security and connectivity architecture**.

What you can do

- Ask your security vendors for implementation of advanced **HOBsec functionality** (we will gladly help them out).

Summary

- New, extended concepts for secure connectivity products will
  - add visibility and control for enterprises.
  - improve user satisfaction by providing transparency and control.
- The new generation of connectivity tools will
  - complement security products by extending their capabilities into the endpoint devices and
  - help users control their individual digital ecosystems.

Summary

better Security + better Connectivity =

HOB Secure Connectivity

www.hobsoft.com

Visit our booth **#3535** in the North Expo