Case Studies, Lessons Learned

Ing. Tijl Deneut
Lecturer Applied Computer Sciences Howest
Researcher XiaK, Ghent University

UNIVERSITEIT GENT

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

KU LEUVEN

XiaK

Case Study Overview

3 different types of cases

- Troubleshooting
  - "We have systems shutting down, why exactly?"
- Implementation
  - "We want to adapt our network, can you assist?"
- Security
  - "Is this secure and why not?"

Troubleshooting Case Studies

Usually, we start capturing network data and with the resulting PCAP files, we try to find the problem and provide recommendations

Example Case Studies:

1. Cogeneration (*WKK*) generates false positive messages: alarms were received about emergency buttons pressed that weren't pressed

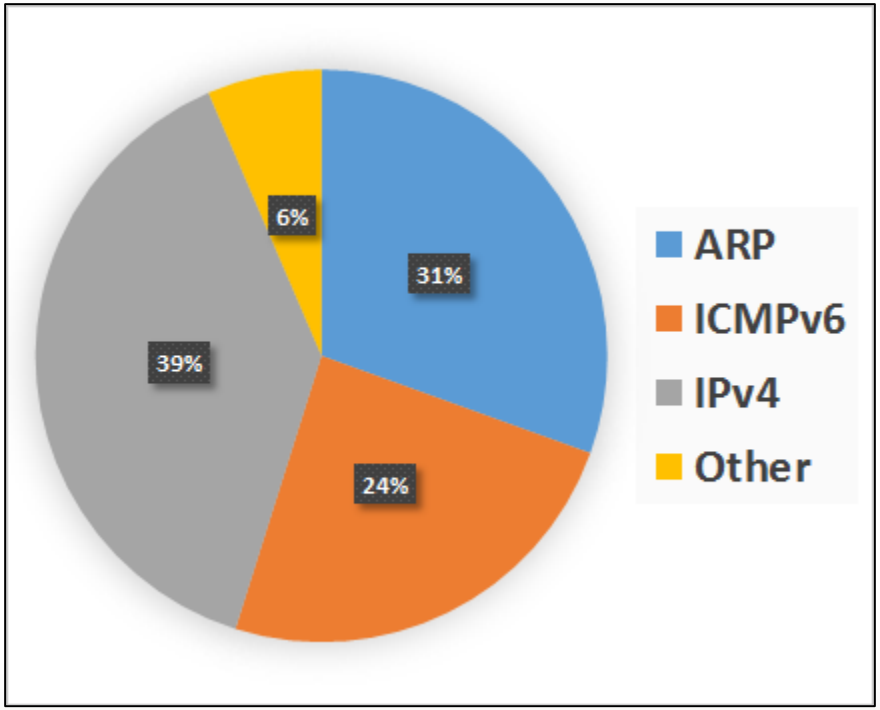
   Presented on 2015-05-07

2. PLC switches to STOP Mode every day because of abnormal large TCP packets being broadcasted

   Presented on 2016-03-15

Lessons Learned Troubleshooting

A common factor with troubleshooting was the amount of unnecessary traffic



Implementation Case Studies

General case: companies migrating from a certain network layout to a better layout.

Besides assistance we try to take captures **before** the migration and compare them with captures taken **after** the migration.

Example Case:

- Migration from a flat network to fully VLAN'ed network with interVLAN routing

  Presented today

Implementation Case Study

Company had a large and mostly “flat” network

- This means every device can connect directly to every other device. No intermediary routers
- The network traffic looked similar to that in the troubleshooting cases, so lots of broadcasts
- How do we implement network enhancements to prevent future problems?

- Used VLANs: not just separating the Office from the Production network, but creating a network **per machine**

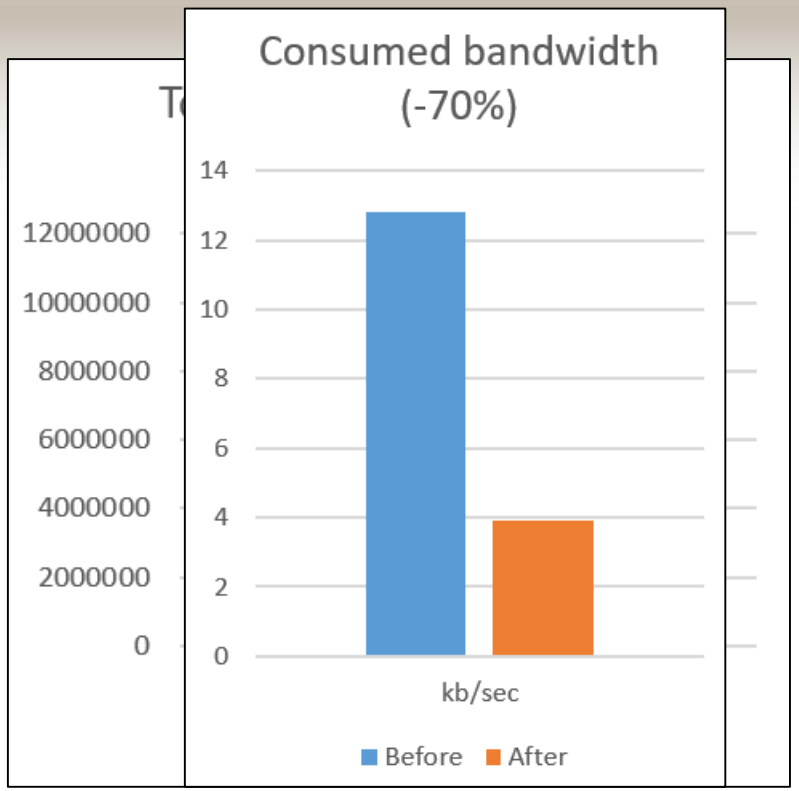
Data gathered (raw)

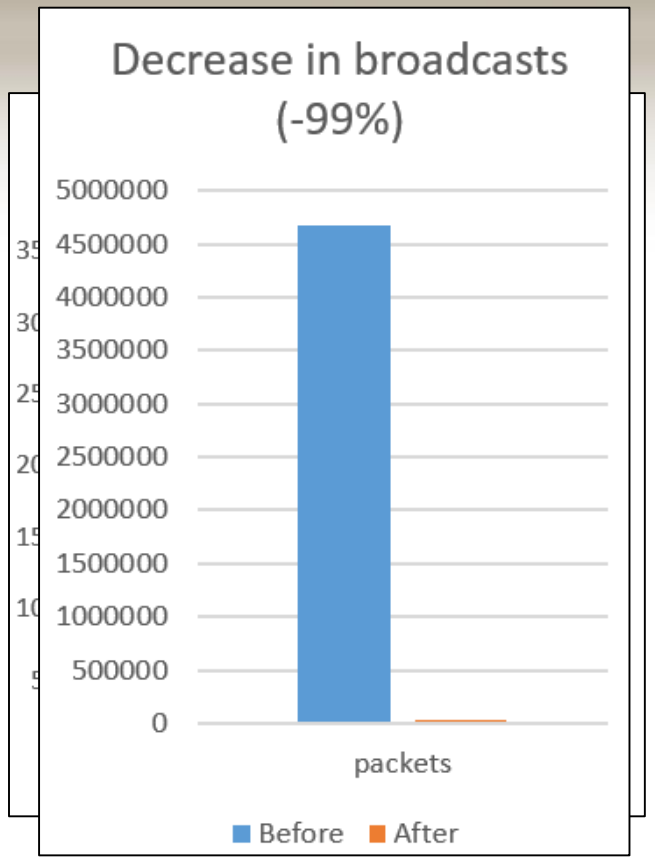
Statistics from data gathered at the **entry** of one (large) machine (over a period of **exactly** 24 hours)

- 90% decrease in total packets sent over the network
- 90.2% decrease in average packets/sec
- 207. 9% increase in average packet size, optimizing network I/O by sending small packets less frequently, avoiding connection establishment overhead
- 69.7% decrease in average used bandwidth
- 75.7% decrease in ARP table size
- 99.4% decrease in total broadcast packets

Alexander Van Maele

Lessons Learned
Segmentation Results





UNIVERSITEIT GENT

howest De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

Security Case Studies

Larger vendors and companies requesting various audits and research

1. Confirmed several security bugs in current ICS hardware and resolved them, for BECKHOFF
   Presented on 2015-12-03 and 05-07 and …

2. Brand new hardware "*pen*" tested for SIEMENS
   → *Presented today*

3. Assist in secure Remote Access ICS setup **in the field**
   → *Starting phase, presented today*

UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN XiaK

Beckhoff Case Study overview

- Both the Beckhoff CX9020 PLC as well as the CP6066 suffered from the same vulnerability in their website (*http://<ip>/config*) that allowed **Unauthenticated Access** and eventually **Remote Code Execution**
- After consultation with the German Beckhoff engineering department a **Software Update** was released mid August 2015 that fixes these issues

Technical details: CVE-page / Firmware update

Exploit script: http://www.github.com/tijldeneut

UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN XiaK

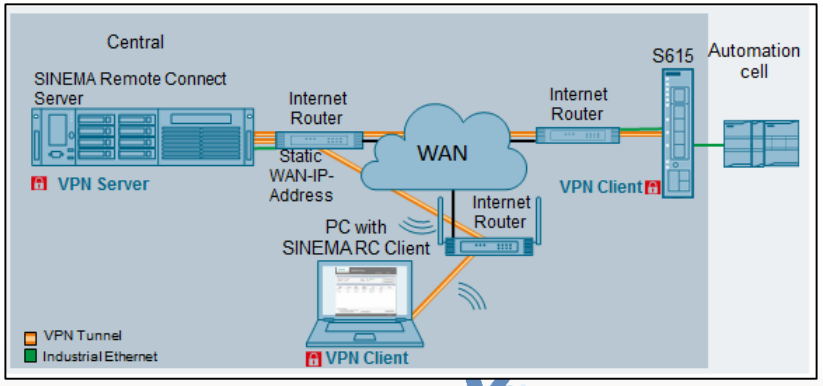
Siemens Case Study overview

Security Investigation on Scalance S615

- Newest **SINEMA Remote Connect** router
- Built specifically for secure VPN connections using a companion software a.k.a. Virtual Machine (Debian)

Results

- Investigating the Router webserver showed no security problems
  - E.g. when opening it the first time, the password **must** be changed to a **strong** password
- VPN Tunnel research is ongoing, but OpenVPN (especially when using **signed** certificates) is a very good choice!
- Fuzzing several services did not cause any problems
  → Using off-the-shelf Linux Distributions can be a big plus, e.g. for updates



UNIVERSITEIT GENT

howest De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

Siemens Case Study Results

Only Good news? Almost ☺

- The delivered Firmware had SNMP enabled with the default community string *public*.
  As previously demonstrated, this could be an information disclosure problem

  → However, when performing a **firmware update** and restoring the factory defaults, we learned this was no longer the case.

- A different problem would be the Profinet Discovery protocol (aka *PN_DCP*). This router, just like most industrial Siemens hardware (and software) we know off, responds to PN_DCP Get ánd Set packets.
  This allows for unauthenticated read and write of e.g. the network settings.

  → Enabled by default, this behavior cán be disabled on this router.

UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN XiaK

New Case Study (April 2016)

- Assisting in configuring a **Remote Access** scenario where a PLC needs to be accessed by **End Users** in a secure way
- Including access from mobile devices
- Including separate technical access pages

UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN XIAK

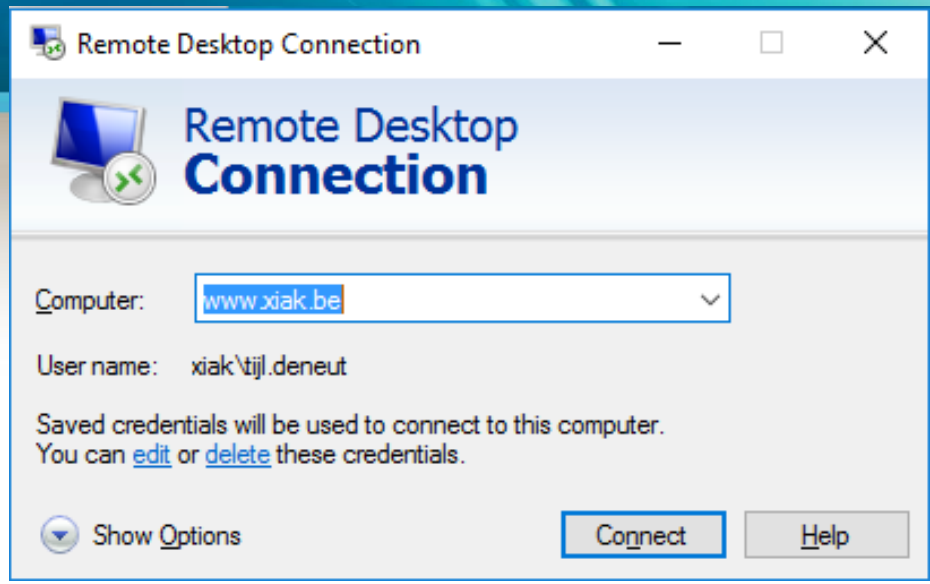
Security Case Studies continued …

Certain research cases were requested by **several companies:**

- "Please investigate TeamViewer security"
  Resulted in a script+article as presented on *2015-12-03*

- "Please investigate Microsoft Remote Desktop security"
  Presented today

Remote Desktop Protocol



- Technique for taking over a Windows PC remotely
- Client is present on every Windows version since XP (mstsc.exe)
- Supports a lot of features:
  Copy-Paste, File System & Audio Redirection, Printer & Port Redirection

UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN Xiak

RDP Security Features 1

- Since 2006, RDPv6 supports RC4 cipher for encryption, still supported up to today
  - This means XPSP2, 2003SP1 and later
  - Still supported by most recent RDP clients **today**
  - Older server versions (<=v5.2) are **no longer supported** since 2012 (Win8 & Server2012), so encryption is always present as of 2012

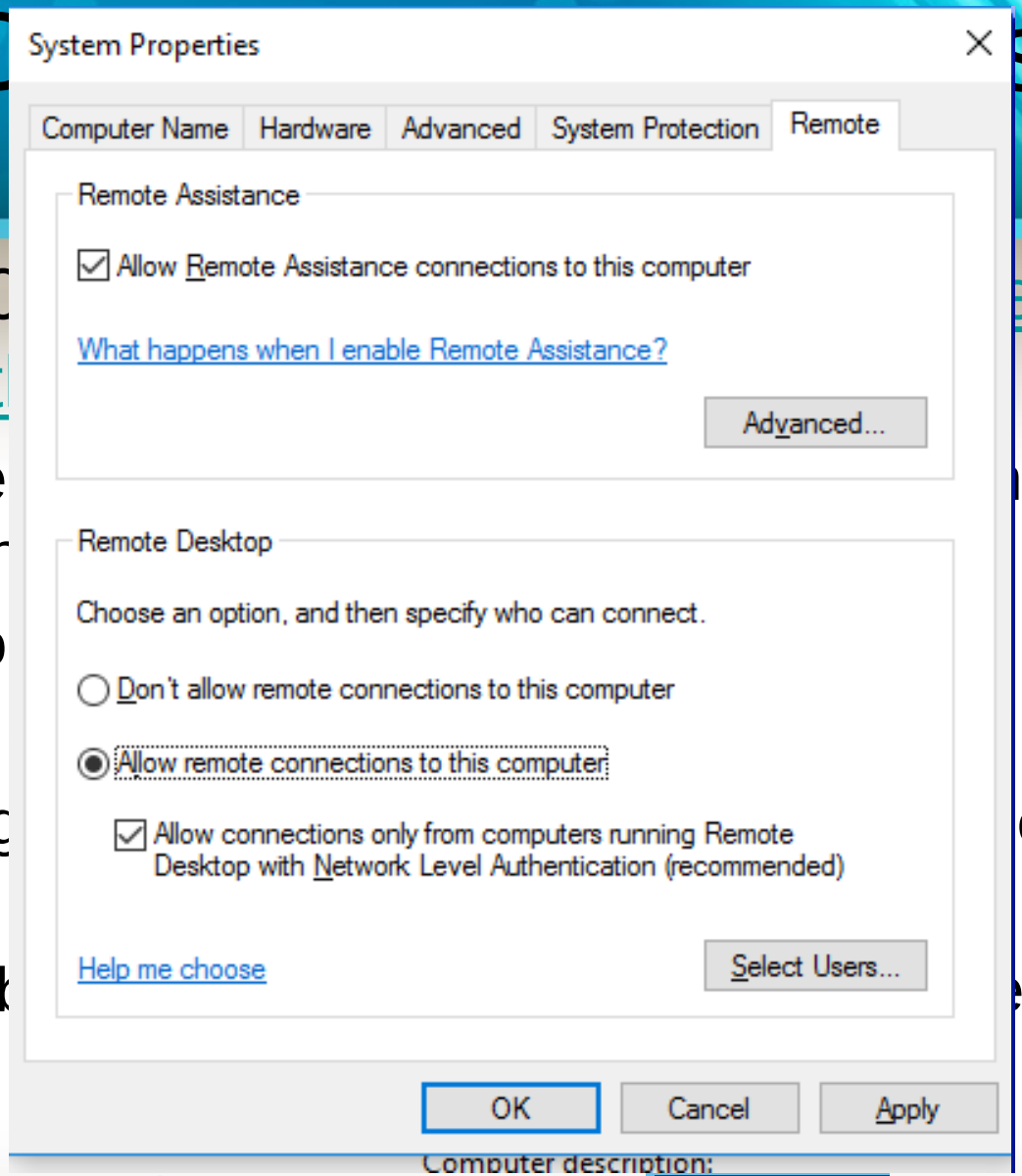
→ RC4 is insecure, but difficult to decrypt in real-time

RD … s 2

- Since 200… …etwork Level Aut…
  - Uses se… …e TLS1.0 cipher, r…
  - Only wo… …later and client is …

→ This is neg… …e enabled on the **Server**

→ **Not possib**… …nts



Known Security Issues

- Oldest RDP implementations have no encryption, so easy Man-in-the-Middle would reveal credentials
- All RDP sessions are susceptible to in-memory credential harvesting (Kerberos passwords in *lsass.exe*)
- MS12-020/CVE-2012-0002 DOS vulnerability (March 2012)
  → Crashes the client without the need for credentials, public code available
- MS15-067/CVE-2015-2373 vulnerability (July 2015)
  → No public code available (yet)

But there is more …

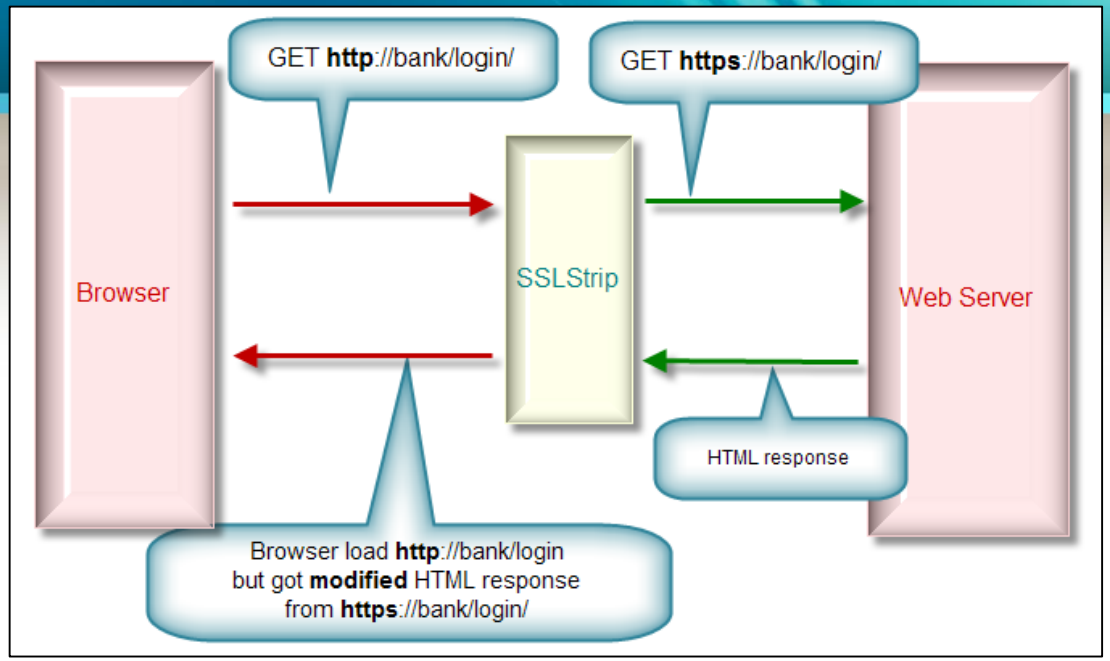
- Let's get back to the Man in the Middle option:

- When an RDP session is started, there is always a **negotiation phase** between the client and the server. In this phase the server usually sends his public certificate to the client who uses that to encrypt all further data.
- This negotiation can result in one out of three types of connection types:
  - RDP Security Layer: Native encryption, only possible with AD
  - CredSSP: SSL with NLA, separate proprietary protocol
  - SSL: TLS 1.0 or RC4 with PKI using certificates

The pitfall

- Both last options will result in this Accept Window
- Our attack will result in **replacing** the public SSL certificate issued by the server with one of our own
- In short: we can **strip** the SSL certificate from the connection (ssltrip)

Is this brand new?



- Not for HTTP (sslstrip)
  - But this is RDP
- Not for RDP either
  - The old Windows tool *'Cain & Abel'* supports RDP sniffing
    - But buggy, unreliable and only for older RDP versions

What is new?

rdpstrip.py

→ Accepts RDP connections and forwards them to a server

- Requirements: Python
- Works on: Windows & Linux

- 3 modes:
  - Sniffing mode: just show RDP endpoints, no certificate interception
  - Forward: client connects to hacker, requires only server IP
  - Mitm: rdpstrip.py will also perform ARP Poisoning, requires server and client IP (Linux Only)

So what's so special?

The output!

The scripts parses all data as it passes by

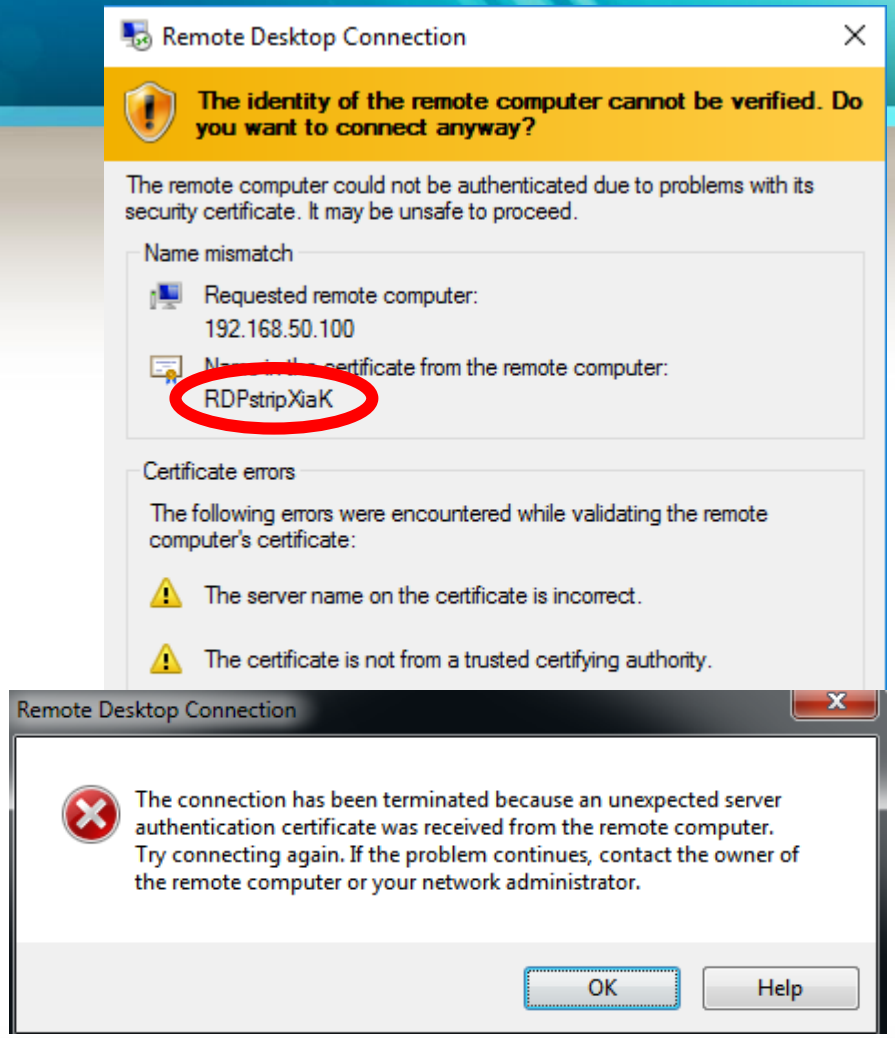
- Credentials and interesting information are captured and stored in a log file
- All keystrokes are also captured and stored in a separate log file
- A PCAP file (Linux only) is made with all captured and unencrypted data

Show me

Demo

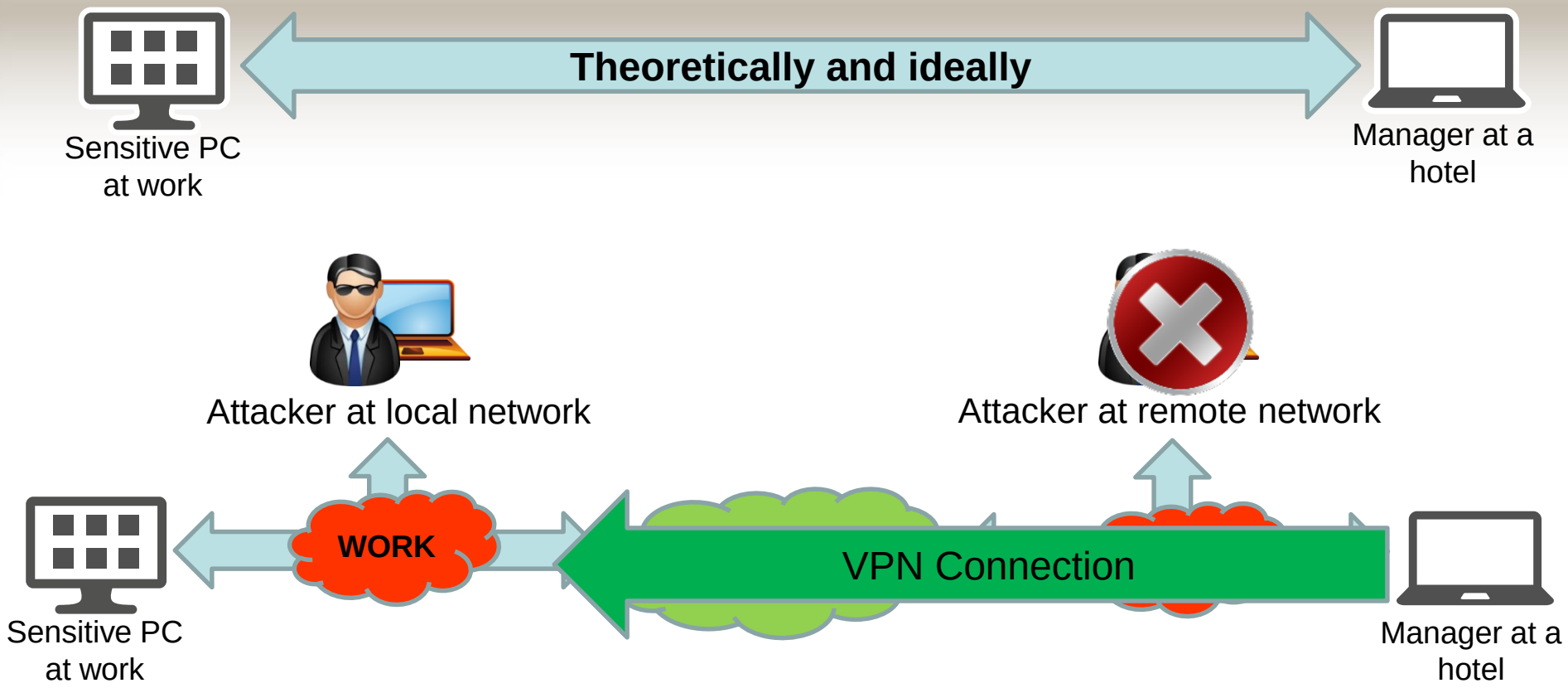
What did we discover?

- The displayed certificate Window differs a little bit
  - This is however configurable and thus fixable
- Jumping into an established session actually returns an error message
- Unless you are using **Third Party** tools (mRemote!)



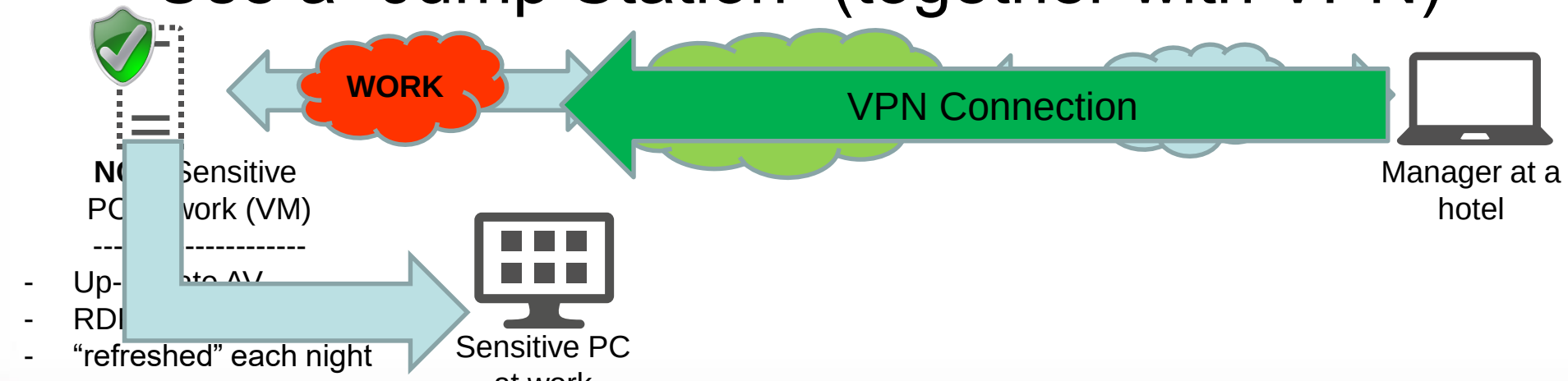
UNIVERSITEIT GENT howest De Hogeschool West-Vlaanderen KU LEUVEN XiaK

Why should we care?



Best solution?

- Switch to the newest RDP version
  (where possible)
- Enable Network Level Authentication
  (where possible)
- Use a “Jump Station” (together with VPN)



- Up-
- RDI
- “refreshed” each night

Questions?

New case studies or challenges are still welcome

"The key to life is accepting challenges. Once someone stops doing this, he's dead."
— Bette Davis