**WikiLeaks and the CIA's hacking secrets, explained**

A WikiLeaks data dump claims to detail ways in which the CIA could hack your devices, including phones, computers and TVs

<https://www.cnet.com/how-to/wikileaks-cia-hack-phone-tv-router-vault-7-year-zero-weeping-angel/>

### Class Material 2017-01-18

Attached Files:

* [[File](https://mygateway.umsl.edu/bbcswebdav/pid-3782678-dt-content-rid-24384830_1/xid-24384830_1) 2017-01-18\_1.pptx](https://mygateway.umsl.edu/bbcswebdav/pid-3782678-dt-content-rid-24384830_1/xid-24384830_1) (1.113 MB)
* [[File](https://mygateway.umsl.edu/bbcswebdav/pid-3782678-dt-content-rid-24384831_1/xid-24384831_1) 2017-01-18\_2.pptx](https://mygateway.umsl.edu/bbcswebdav/pid-3782678-dt-content-rid-24384831_1/xid-24384831_1) (1.483 MB)

[2017-01-18\_1.pptx](https://mygateway.umsl.edu/bbcswebdav/pid-3782678-dt-content-rid-24384830_1/xid-24384830_1)

Volt 7 (2013-2016)

Malware and Viruses

IOS, MS Windows, Google Android

Smartphone Location, and messages

Controls phones, microphone and vehicle control systems

Once they are hacked, they have full access as if they used your thumbprint or access code

Apple says they are fully secure with their latest updates

Android and Windows are still looking into the documents

They can get into a specific target phone, camera, TV’s

Whereas, snowdens version goes on the corporate servers and drags a massive net across and collects massive amounts of data

<https://threatpost.com/>

<http://www.theregister.co.uk/security/>

Online sources I like

http://www.csoonline.com/blogs  
http://www.forensicmag.com/news  
https://www.f-secure.com/weblog/  
http://blog.imperva.com/  
http://www.krebsonsecurity.com/  
https://blogs.mcafee.com/category/mcafee-labs/  
http://www.net-security.org/secworld\_main.php  
http://www.databreaches.net/  
https://packetstormsecurity.com/  
http://blogs.rsa.com/  
http://searchsecurity.techtarget.com/#

http://www.symantec.com/security\_response/  
http://www.theregister.co.uk/security/  
https://threatpost.com/  
http://blog.trendmicro.com/  
https://www.us-cert.gov/ncas/current-activity  
http://arstechnica.com/security/  
http://www.cnet.com/topics/security/  
http://slashdot.org/stories/security  
http://blogs.technet.com/b/msrc/  
https://www.privacyrights.org/data-breach  
https://www.sans.org/newsletters/newsbites/  
https://isc.sans.edu//  
http://www.securitytracker.com/

Welcome to  
IS 3878/6878!

IS 3878/6878: Management of information security

Spring 2017

Kurt Aubuchon

Discussion Topics

Introduction of the instructor

Introduction of students

Overview of the class

Expectations for Risk Analysis assignments

Expectations for Term Project

Quizzes and Exams

Welcome to St. Eligius!

Who is this guy?

~17 years experience in IT

~10 years in security

Healthcare, Fortune 100, higher education

Experience as the Information Security Officer at a large healthcare organization

Currently\* work for Hunter Engineering as Director of Information Security

CISSP, CISM, CCE, CEH, CHFI

BA, English Literature, William Jewell College, 1995

MBA, University of Cincinnati, 2008

(\* as of 1/23)

Who is this guy?

Email: aubuchonku@umsl.edu

Cell: 573-214-1454

Calling or texting is OK, but my response may be a little slow.

I have a day job and two small children, but I will make every effort to respond promptly.

Evenings between 6:00 PM and 8:30 PM, I’m usually spending time with the kids, so if you call/text then, I probably won’t get back to you till after the kids are asleep.

Please no calls/texts between 10:00 PM and 6:00 AM.

www.linkedin.com/in/kurtaubuchon

kurtaubuchon.blogspot.com

Who are you?

What is your full name (so I can find it on the roster)?

What do you like to be called?

What experience, if any, do you have working in the information security field?

What do you hope to get out of this class?

Give one reason why you think security breaches seem to be so prevalent.

Class Overview: Topics

This Class Is About:

Systematic management of information security

Integrating information security into the business

Information security governance

Risk management

Legal and regulatory compliance

Ethics in information security

Incident response

It is NOT About:

Technical, hands-on skills

Tactical information security configuration and controls

Preparation for a certification (although it is organized according to the CISM domains)

Assignments & Grades

Eight Risk Analysis papers

Combined 25% of your grade

One Term Project

25% of your grade

Two exams

25% of your grade, each

Three or four Unit Quizzes

Ungraded; for practice and self-assessment

Risk Analysis Papers

As a professional information security analyst, you will routinely be required to assess the risk of a newly disclosed vulnerability, a recently active threat source, a particular attack technique, etc. The way this usually works is that a news story hits the information security press or the general business press, and your manager instructs you to research the details and produce an executive level assessment of the risk to the organization. You then will have a short period of time (usually no more than a business day) to delve into the story, get down to the facts, and produce an actionable assessment for your leadership.

In a professional setting, your work product will usually be in the form of a *brief* document or email, the equivalent of no more than one typed page. It will summarize the key points of the issue, describe how (if) it might impact your organization, and recommend steps to mitigate the risk in the short term and long term.

Risk Analysis Papers

In this class, you will be taking the role of an Information Security Analyst or Information Security Architect at our mock employer, St. Eligius Healthcare (see the details of St. Eligius later in this deck). When a big story hits the information security press, you will be asked to research it and produce an analysis for St. Eligius’s CISO. Which is me.

For each assignment, I will be expecting a one-page paper in Word, PDF, etc., format that includes the following:

A summary of the issue

A description of the potential impact to St. Eligius

Short term or stop-gap mitigation steps

Long term mitigation

Risk Analysis Papers

Step 1

Review articles published in the information security press or general press. Look for reports of security issues that may pose risks to St. Eligius.

In a professional setting, you will be reacting to reports very quickly as they come out. However, for the purposes of this class, you may use older articles. Please do not go back more than a year.

There are many online sources you can use to learn about new vulnerabilities and risks. Some that I like are listed on the next page, but feel free to use other sources as well.

Risk Analysis Papers

Online sources I like

http://www.csoonline.com/blogs  
http://www.forensicmag.com/news  
https://www.f-secure.com/weblog/  
http://blog.imperva.com/  
http://www.krebsonsecurity.com/  
https://blogs.mcafee.com/category/mcafee-labs/  
http://www.net-security.org/secworld\_main.php  
http://www.databreaches.net/  
https://packetstormsecurity.com/  
http://blogs.rsa.com/  
http://searchsecurity.techtarget.com/#

http://www.symantec.com/security\_response/  
http://www.theregister.co.uk/security/  
https://threatpost.com/  
http://blog.trendmicro.com/  
https://www.us-cert.gov/ncas/current-activity  
http://arstechnica.com/security/  
http://www.cnet.com/topics/security/  
http://slashdot.org/stories/security  
http://blogs.technet.com/b/msrc/  
https://www.privacyrights.org/data-breach  
https://www.sans.org/newsletters/newsbites/  
https://isc.sans.edu//  
http://www.securitytracker.com/

Risk Analysis Papers

Step 2

Read information from multiple sources. Make sure you understand the underlying technical issues. Write a brief summary of the issue (usually no more than a paragraph). Include links to your sources so I can get more details if I want them.

*Example:*

On March 27, security researchers at Imperva released a [paper](http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf) describing a new attack on SSL/TLS encrypted data.  The attack exploits a 13-year-old vulnerability in the RC4 cryptographic algorithm.  The paper shows how the "vulnerability can be used to mount several partial plaintext recovery attacks on SSL-protected data when RC4 is the cipher of choice, recovering part of secrets such as session cookies, passwords, and credit card numbers."  Unlike other SSL attacks that require the attacker to intercept the targeted traffic via a Man-In-The-Middle attack, this new attack only requires that the attacker is able to passively sniff the traffic.  The attack has been nicknamed the "Bar Mitzvah Attack" in reference to the 13-year-old vulnerability it exploits.

Risk Analysis Papers

Step 2

Note that the example gave enough detail for a reasonably technically-sophisticated executive to grasp the key points quickly. It includes a link to the source report. You may assume the audience for your analysis has some technical background but may not be a hands-on technician. You can include links to security articles and technical documents as you feel necessary.

(Don’t link to Wikipedia. There is good information there, but if you use it as a primary source you’ll look like a bozo in front of your boss.)

Risk Analysis Papers

Step 3

Look at the details of the St. Eligius environment. Determine what impact the issue will have on St. Eligius’s security posture.

If your assessment is that the issue poses no risk to St. Eligius, that’s perfectly acceptable, as long as you can justify that assessment persuasively. **For the purposes of this class, don’t pick a “no risk” issue for more than one of your assignments**.

St. Eligius is a mock organization. I’ve sketched it out, but I’ve left the details deliberately vague. If you need St. Eligius to have a certain technology so you can write your assignment, you can assume it does. For example, if you want to write about an Oracle vulnerability, you can assume St. Eligius’s EMR is sitting on a nice big Oracle database. As long as it’s a reasonable assumption, I’ll accept it.

Risk Analysis Papers

Step 3

Write a paragraph or so relating the issue to St. Eligius specifically. What does this story mean for us right now? Point out the assets, applications, business processes, etc., that are implicated.

Describe the risk to St. Eligius objectively. Describe the *business impact*. Be realistic and measured. Not every vulnerability poses an existential threat to the organization.

Risk Analysis Papers

Step 3

*Example:*

RC4 has been considered a weak algorithm for several years and is in the process of being phased out. However, it is often maintained on servers to provide backward compatibility with older browers. Approximately 30% of TLS communication uses RC4 ([see here](http://www.darkreading.com/attacks-breaches/ssl-tls-suffers-bar-mitzvah-attack-/d/d-id/1319633)). Any of St. Eligius’s TLS-based applications that continue to support RC4 are vulnerable. Attacks against the vulnerability may expose confidential data including login credentials, patient health data, and financial data. Because exploits for this attack are easily available, the likelihood of a successful attack against St. Eligius is high.

Risk Analysis Papers

Step 4

Write a paragraph or so outlining the steps we should take in the short term. We’re not going to implement a major technical control in the next day or two. So, what controls can we realistically put in place to reduce our risk today?

*Example:*

All TLS-based applications in use at St. Eligius should be assessed to determine if they support RC4. Application owners should determine the business impact of disabling RC4 and should develop a plan to disable it promptly, in accordance with standard change management procedures. The Information Security Office should provide guidance and track all changes to completion.

Risk Analysis Papers

Step 5

Write a paragraph or so outlining the long-term fix for the issue. What do we need to plan for in the future to make sure we have an effective, sustainable, scalable control in place for this? In some cases, you may not need to, or be able to, implement a “big fix”. The short term-mitigation might be your permanent fix. That’s OK, as long as you can support that assessment.

*Example:*

St. Eligius’s internal development standards should be revised to eliminate RC4 as a supported algorithm from all future in-house development projects. Server and application on-boarding processes should be revised to ensure that RC4 is disabled on all new systems prior to their being placed in production.

Risk Analysis Papers

Any questions on the Risk Analysis Papers?

Term Project

As a professional information security analyst, you will often participate in drafting proposals for major information security projects. Your employer may be considering implementing a major new control, such as an endpoint security system, SIEM, DLP, etc. Or, your employer might be considering abandoning a control it already has in place. For example, some organizations today are re-evaluating the need for traditional antivirus solutions. Any major decision such as this will be analyzed and discussed at a high level.

In the professional setting, the information security function will analyze the environment and the available options and will produce a proposal to be presented to the organization’s executive leadership. This proposal will often be part of the CISO’s budget request for the coming years.

Term Project

When the security team is asked to produce a proposal for a major security implementation, the deliverable will typically be one or more slide decks. The decks will be used to try to persuade the organization to implement the new control, to explain the impact on the organization’s current business processes, and to compete for funding during the budgeting cycle.

In a professional setting, this type of effort will usually be done by a team. In this class, you will do it as an individual assignment.

Often these presentations take the form of a number of slides which will be used during a speaking presentation, followed by a number of “backup slides” that have detailed data exhibits and references the speaker can call on if necessary or direct the audience to for further information. The “backup slides” contain all the data that supports the arguments presented in the slides the speaker uses in the presentation.

Term Project

As an Information Security Architect at St. Eligius Healthcare, you are asked to analyze a major security project and produce materials that the CISO (me) will use to argue for its implementation. (Later in this deck there are several suggested projects you can choose from, but you’re not required to pick off that list).

The CISO has an hour to make a case for this project in front of the CIO and all the other senior IT execs. So, you need to give me a deck I can get through in an hour. It needs to have enough supporting data in backup slides that I can support the argument when the other execs challenge me.

The deck needs to be persuasive in terms of *business needs*. It’s not effective to say a control is “best practice”. You need to build a case for why the control will support our business.

Term Project

Expectations

A persuasive, professional-looking slide deck.

Attractive appearance is important, but it needs to be professional, not “cute”.

Something that’s reasonable to deliver in about an hour. So, maybe 30-40 primary slides.

Ample backup slides showing me your work. How did you arrive at your recommendation, what data did you gather, what data supports your argument that this control will manage risk.

If you are recommending a specific product, **demonstrate that you considered at least three alternatives** before settling on the one you’re recommending.

Term Project

Expectations

If you are recommending the implementation of a control, you need to tell me the value of it as well as how we’re going to maintain it for 3-5 years. Consider:

Costs to implement: hardware, software, staff time, etc.

Risks reduced, losses avoided, etc.

Ongoing monitoring and metrics.

Affect on end users, business operations, customers, partners, etc.

Ongoing costs of operation (“care and feeding”).

Staff to maintain and operate it.

Scalability as the organization grows.

How changes will be managed and implemented.

Legal and regulatory implications.

Term Project

Expectations

Since this is not a real scenario, we do not have real budget numbers to work with. And vendors may not be forthcoming with their costs. I understand there will be some fudging for the purposes of the exercise. You can do any of the following:

Make some assumptions and estimate budget numbers that seem reasonable.

Use placeholder variables. Show me how you would calculate the costs and savings, but just use variables where there would be numbers if you had them.

Use real-world numbers if you can get them.

Express costs and savings as percentages of current state (e.g., “implementing this tool will reduce staff required for access provisioning by 10%”.)

Term Project

You Will Be Graded On:

The thoroughness of your analysis

The soundness of your argument

The presentation of the content in the deck

Tips:

This is a LOT of work. Don’t wait till the last week to do it.

We will use a couple of class sessions to check everyone’s progress and help you stay on track. Come to these sessions prepared to ask questions and discuss where you are.

*Come to me for help if you’re stuck! I want you to do well on this!*

Term Project

Project ideas (these are just suggestions – feel free to come up with your own)

Implementing a Data Loss Prevention (DLP) solution

Implementing a Security Information and Event Management (SIEM) solution

Implementing a comprehensive security awareness and education program

Engaging a full-scale penetration test, with plans for periodic re-testing

Implementing database encryption

Abandoning traditional desktop antivirus and replacing with another solution

Implementing a File Integrity Monitoring solution

Implementing an Application Whitelisting solution

Implementing Full Disk Encryption

Removing Local Administrator privileges from end users

Exams and Quizzes

There will be two exams. Each will be about 50-75 questions, multiple choice.

The questions will come from the lectures, case studies, and assigned readings.

There will be three or four (depending on time) “unit quizzes”. These are ungraded (I’m not even going to collect them). I encourage you to view these as an opportunity to assess your understanding and guide your study priorities.

The questions on the unit quizzes will be similar to those on the exams.

St. Eligius Healthcare

Congratulations! You are now an Information Security Architect at *St. Eligius Healthcare*! You will be reporting to the CISO, Kurt Aubuchon. He’s a burnout who wants to quit his job and join the circus. Do well, and you might be next in line for his job when he implodes!

Following this slide are organizational charts and network diagrams that will hopefully give you enough information to complete your assignments. However, this is a mock environment. I’ve sketched it out, but I’ve left the details deliberately vague. You can fudge and improvise if necessary, as long as it fits the general scenario. For example, if you want to write about an Oracle vulnerability, go ahead and assume St. Eligius’s EMR is sitting on a nice big Oracle implementation. As long as it’s a reasonable assumption, I’ll accept it. If you’re in doubt about whether you can make a certain assumption, just ask me.

St. Eligius Overview

Medium-sized healthcare organization in a two-state region.

Four hospitals, three outpatient surgery centers, 20 physician offices, five mobile offices (health screening vans, etc.).

Affiliated with a local medical school

About 15,000 employees

Non-profit

St. Eligius Organizational Chart (partial)

St. Eligius Infrastructure Overview

St. Eligius Network Diagram (partial)

St. Eligius Network Diagram (partial)

St. Eligius Network Diagram (partial)