COM3020J: Info Security for Internet of Things Course Information

Dr. Anca Jurcut
E-mail: anca.jurcut@ucd.ie

School of Computer Science and Informatics
University College Dublin

Beijing-Dublin International College

About me

- I was born in Romania and I moved to Ireland in 2007, after awarded with a PhD Scholarship.

- I am an Assistant Professor in School of Computer Science and Informatics in UCD as part of the BDIC program
- Before, I taught and I did research in the University of Limerick and I worked for IBM Dublin, Ireland
- Last semester it was my fourth time being in China!

About Me

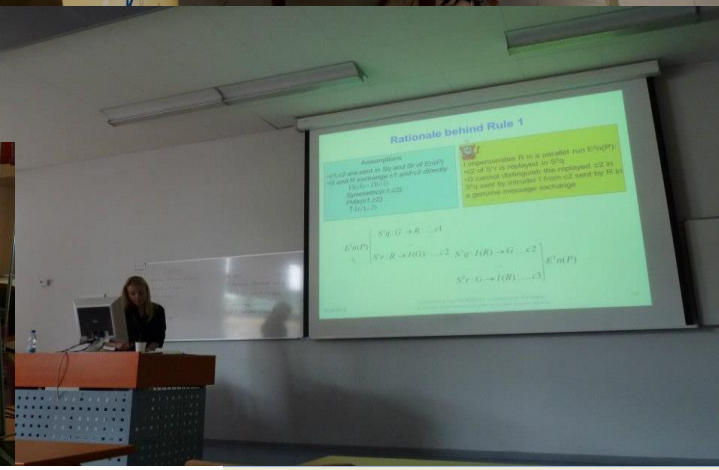
- I did my PhD in University of Limerick (Ireland), in the area of Data and Network Security.
  - I do research in Security Protocols Analysis, Logic-based Verification Techniques, Cryptography, Automation of Logics used in Formal Verification, Theorem Proving Techniques and Mathematical Modelling

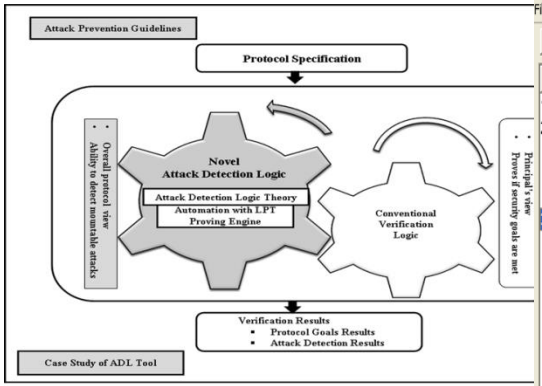
- Previously taught in:
  - West University of Timisoara, Romania
  - University of Limerick, Ireland
  - University College Dublin, Ireland
  - Oulu University, Finland

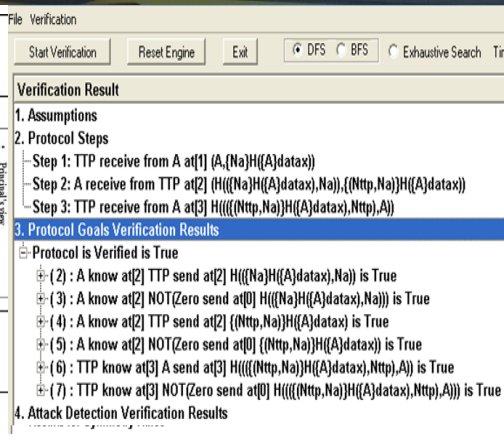

International Conference
Computer Networks


Microsoft


JOURNAL OF COMMUNICATION
Certificate of Completion
Anca Iurcut


Rationale behind Rule 1


Attack Prevention Guidelines
Protocol Specification
Overall protocol view
Ability to detect countable attacks
Novel
Attack Detection Logic
Attack Detection Logic Theory
Automation with LPT
Proving Engine
Conventional
Verification
Logic
Principal's view
Proves if security goals are met
Verification Results
Protocol Goals Results
Attack Detection Results
Case Study of ADL Tool


File Verification
Start Verification
Reset Engine
Exit
DFS
BFS
Exhaustive Search
Verification Result
1. Assumptions
2. Protocol Steps
Step 1: TTP receive from A at[1] {A,{Na}H({A}datax)}
Step 2: A receive from TTP at[2] {H({{Na}H({A}datax),Na}),{(Nttp,Na)}H({A}datax)}
Step 3: TTP receive from A at[3] H({{{{Nttp,Na)}H({A}datax),Nttp),A)}
3. Protocol Goals Verification Results
Protocol is Verified is True
{2} : A know at[2] TTP send at[2] H({{Na}H({A}datax),Na)} is True
{3} : A know at[2] NOT(Zero send at[0] H({{Na}H({A}datax),Na)}) is True
{4} : A know at[2] TTP send at[2] {(Nttp,Na)}H({A}datax) is True
{5} : A know at[2] NOT(Zero send at[0] {(Nttp,Na)}H({A}datax)} is True
{6} : TTP know at[3] A send at[3] H({{{{Nttp,Na)}H({A}datax),Nttp),A)} is True
{7} : TTP know at[3] NOT(Zero send at[0] H({{{{Nttp,Na)}H({A}datax),Nttp),A)}) is True
4. Attack Detection Verification Results

Course Overview

- Description:
  - We will cover selected security topics in each of the following areas:
    - Cryptography
    - Access control
    - Protocols
    - Software

- Course Schedule & Duration:
  - 12 weeks of lecturing (room 203, Teaching Building 3)
    - each Monday (1:30pm)
    - **Now 11 weeks after today!**
  - **Tutorials**: 9:55am in Zhixing Building
    - Starting: Tuesday 11th September
  - One week revision time
  - Exam

Course Grading

- Marking Scheme:
  - Examination 60%
  - Test 20%
  - Homework, quizzes, class participation, and other work assigned 20%
- No make-up tests or quizzes will be given and ***no*** late homework (or other work) will be accepted.
- **Keys to success**: Do the homework and attend the class!
- Cheating will not be tolerated, but working together is encouraged.

Text, Slides & Notes

- No required text
  - but loads of recommended references
- Slides will be on the Moodle:

  https://csmoodle.ucd.ie/
- Logon using your UCD connect account
- Click on **COMP3020J**
- And enrolment key is **“2019COMP3020J”**

Reading

- "**Information Security: Principles and Practice**", 2nd edition, Mark Stamp, (Wiley, May 2011, ISBN-10: 0470626399, ISBN-13: 978-0470626399).
- Academic Papers
- Other useful resources:
  - "Computer Security: Principles and Practice", Global Edition, 3/E, William Stallings and Lawrie Brown, (Pearson, 2015, ISBN-10: 1292066172 • ISBN-13: 9781292066172)
  - "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", Michael Sikorski and Andrew Honig, No Starch Press, 2012. An excellent book for information on reverse engineering (whether for malware analysis or other purposes). Includes many hands-on exercises.
  - "Applied Cryptography: Protocols, Algorithms and Source Code in C", second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9. For better or for worse, in industry, this is *the* standard reference for all things cryptographic.
  - "Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses", Ed Skoudis with Tom Liston, Prentice Hall, 2006, ISBN: 0-13-148104-5. There are many books that claim to provide information on how to foil hackers, but this is by far the best that I have seen. This is an updated version of the original *Counter Hack*, published in 2001.

Plagiarism

- When submitting tutorials and assignments, you should be aware that plagiarism is very serious.

- Any work you submit should be you own work.
  - Copying directly from the internet is not acceptable.
  - Copying your work from a classmate is not acceptable.

- I want to see what *you* know and how *you* would describe or understand the material.

Course Content

- Introduction
- Crypto
  - Crypto Basics
  - Symmetric Key Crypto
  - Public Key Crypto
  - Hash Functions and other topics
- Access Control
  - Authentication
  - Authorization
- Protocols
  - Simple Authentication Protocols
  - Real World Security Protocols
  - Weaknesses and Attacks
- Software
  - Security Vulnerabilities and Malware

COM3020J: Info Security for Internet of Things Introduction

Dr. Anca Jurcut
E-mail: anca.jurcut@ucd.ie

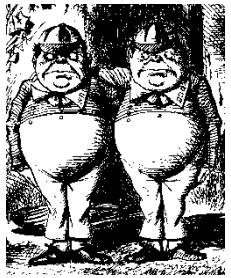
School of Computer Science and Informatics
University College Dublin,
Ireland

“Begin at the beginning,” the King said, very gravely,
“and go on till you come to the end: then stop.”
— Lewis Carroll, *Alice in Wonderland*

The Cast of Characters

- Alice and Bob are the **good guys**

- Trudy is the **bad "guy"** →



- Trudy is our generic "intruder", "attacker"

Alice's Online Bank

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Trudy view the situation?

CIA

- CIA == Confidentiality, Integrity, and Availability
- AOB must prevent Trudy from learning Bob's account balance
- **Confidentiality:** prevent unauthorized *reading* of information
  - Cryptography used for confidentiality

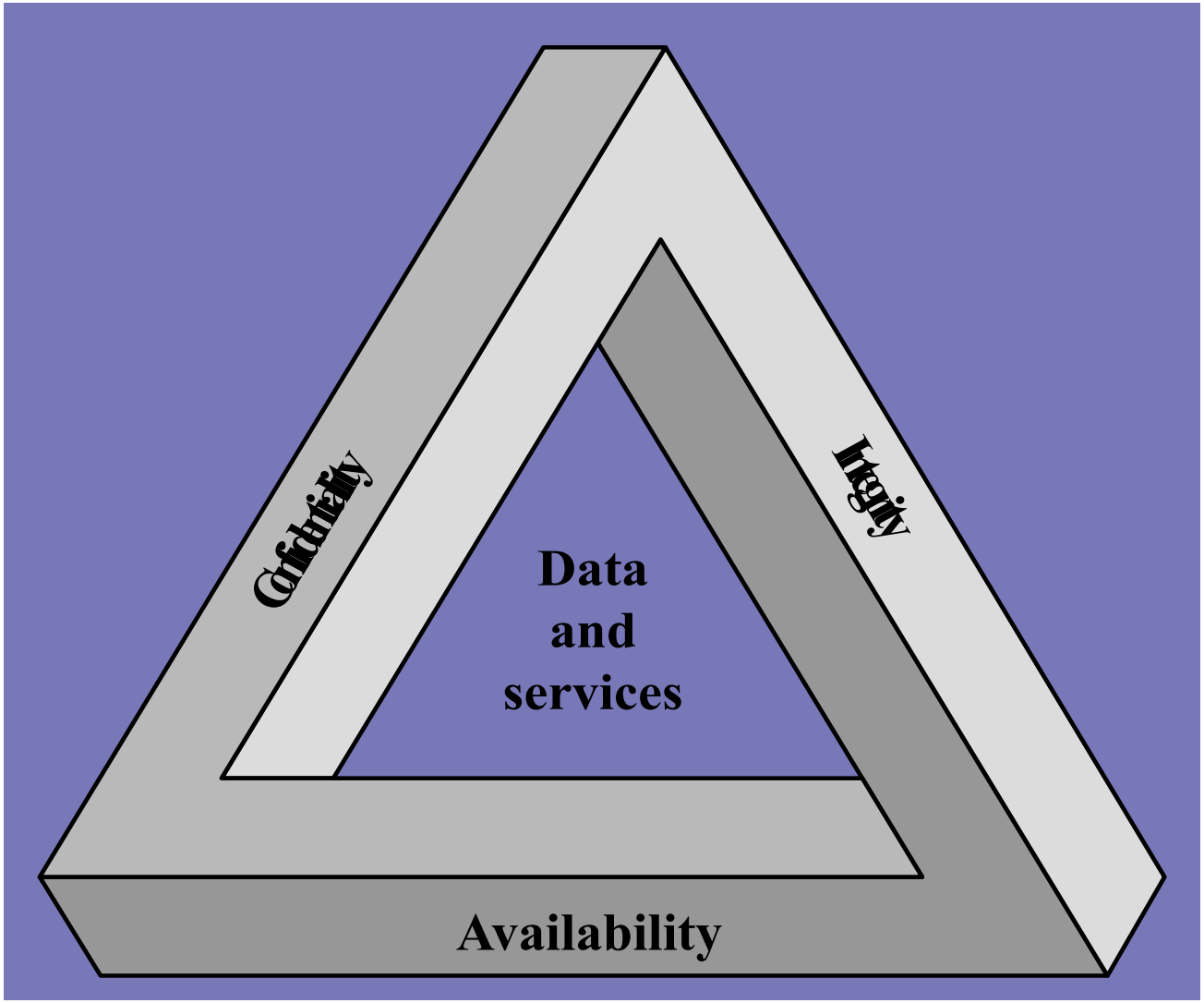
CIA

- Trudy must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- **Integrity:** detect unauthorized *writing* of information
  - Cryptography used for integrity

CIA

- AOB's information must be available whenever it's needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a *timely manner* when needed
- Availability is a "new" security concern
  - Denial of service (DoS) attacks

The CIA Triad



Beyond CIA: Crypto

- How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
  - This requires some clever **cryptography**
- What are security concerns of pwds?
- Are there alternatives to passwords?

Beyond CIA: Protocols

- When Bob logs into AOB, how does AOB know that "Bob" is really Bob?
- As before, Bob's password is verified
- Unlike the previous case, **network** security issues arise
- How do we secure network transactions?
  - **Protocols** are critically important
  - Crypto plays a major role in security protocols

Beyond CIA: Access Control

- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, and so on…
- Enforcing such restrictions: *authorization*
- **Access control** includes both authentication and authorization

Beyond CIA: Software

- Cryptography, protocols, and access control are all implemented in **software**
  - Software is foundation on which security rests
- What are security issues of software?
  - Real-world software is complex and buggy
  - Software flaws lead to security flaws
  - How does Trudy attack software?
  - How to reduce flaws in software development?
  - And what about malware?

This Course

- This course consists of four major parts
  - Cryptography
  - Access control
  - Protocols
  - Software
- We'll focus on technical issues
- But, people cause lots of problems…

The People Problem

- People often break security
  - Both intentionally and unintentionally
  - Here, we consider an unintentional case
- For example, suppose you want to buy something online
  - Say, *Information Security: Principles and Practice*, 2nd edition from amazon.com

The People Problem

- To buy from amazon.com…
  - Your browser uses the SSL protocol
  - SSL relies on cryptography
  - Many access control issues arise
  - All security mechanisms are in software
- Suppose all of this security stuff works perfectly
  - Then you would be safe, right?

The People Problem

- What could go wrong?
- Trudy tries man-in-the-middle attack
  - SSL is secure, so attack does ***not*** "work"
  - But, Web browser warns of problem
  - What do you, the user, do?
- If user ignores warning, attack works!
  - None of the security mechanisms failed
  - But user *unintentionally* broke security

Cryptography

- "Secret codes"
- The book covers
  - Classic cryptography
  - Symmetric ciphers
  - Public key cryptography
  - Hash functions++
  - Advanced cryptanalysis

Access Control

- Authentication
  - Passwords
  - Biometrics
  - Other methods of authentication
- Authorization
  - Access Control Lists and Capabilities
  - Multilevel security (MLS), security modeling, covert channel, inference control
  - Firewalls, intrusion detection (IDS)

Protocols

- "Simple" authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Real-world security protocols
  - SSH, SSL, IPSec, Kerberos
  - Wireless: WEP, GSM

Software

- Security-critical flaws in software
  - Buffer overflow
  - Race conditions, etc.
- Malware
  - Examples of viruses and worms
  - Prevention and detection
  - Future of malware?

Software

- Software reverse engineering (SRE)
  - How hackers "dissect" software
- Digital rights management (DRM)
  - Shows difficulty of security in software
  - Also raises OS security issues
- Software and testing
  - Open source, closed source, other topics

Software

- Operating systems
  - Basic OS security issues
  - "Trusted OS" requirements
  - NGSCB: Microsoft's trusted OS for the PC
- Software is a BIG security topic
  - Lots of material to cover
  - Lots of security problems to consider
  - But not nearly enough time…

Think Like Trudy

- In the past, no respectable sources talked about "hacking" in detail
  - After all, such info might help Trudy
- Recently, this has changed
  - Lots of info on network hacking, malware, how to hack software, and more
  - Classes taught on virus writing, SRE, …

Think Like Trudy

- Good guys must think like bad guys!
- A police detective…
  - …must study and understand criminals
- In information security
  - We want to understand Trudy's methods
  - We might think about Trudy's motives
  - We'll often pretend to be Trudy

Think Like Trudy

- Is it a good idea to discuss security problems and attacks?
- Bruce Schneier, referring to *Security Engineering*, by Ross Anderson:
  - "It's about time somebody wrote a book to teach the good guys what the bad guys already know."

Think Like Trudy

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice's and/or Bob's stupidity
- But, we **cannot** act like Trudy
  - Except in this class …
  - … and even then, there are limits

In This Course…

- Think like the bad guy
- Always look for weaknesses
  - Find the ***weak link*** before Trudy does
- It's OK to break the rules
  - What rules?
- Think like Trudy
- But don't do anything illegal!