



Security Research Group

Spring 2002
Project Overview



Quote of the Day

"I don't know why we are here, but I'm pretty sure that it is not in order to enjoy ourselves."

- Ludwig Wittgenstein (1889-1951)



Areas of Interest

- Security Protocols
- Intrusion Detection
- Cryptography
- Computer Forensics
- Wireless Networks
- Security Education

3



Security Protocols

- Defined: Rules that detail the interaction between parties in a communication that are using cryptography for security.
- Authentication
 - One-way
 - Two-way
 - Second-level
 - Multi-party
 - Non-repudiation
- Privacy/Secrecy
- Nonrepudiation
- Etc.
- Key distribution

4



Simple Protocol

- Goal: Using PGP, securely send a file to a colleague in the CS Department
 - To send:
 - Select the key of the intended recipient
 - Sign and encrypt the secret message
 - Select the email address of the intended recipient
 - Send the encrypted message via email
 - To receive
 - Determine who the message came from'
 - Select the key to match the originator
 - Decrypt the message
 - Check the signature

5



Potential Problems

- What if you get the same message twice?
- How will you know that you got the same message twice?
- How will you know that sent messages are received?

6



The BIG Questions

- Does the protocol produce the expected results when run in a stable, friendly environment?
- Does the protocol produce the expected results when run in an unstable, hostile environment?

7



Simple Protocol

Goal: Two participants are in a session and know that they are both engaged.

– A \rightarrow B: N_a

– B \rightarrow A: $\{N_a\}^k \{N_b\}^k$

– A \rightarrow B: N_b

8



Attack on the Simple Protocol

- Attack session
 - Reference session
1. A -> B: Na
 2. Intruder intercepts
 3. I -> A: Na
 4. A -> I: {Na}k{Na'}k
 5. I -> A: {Na}k{Na'}k
 6. A -> I: Nb

9



Result of the Attack

- Alice believes that she is in a secure session with Bob, but Bob is not involved and is not aware that there is a session.

10



Goal of Protocol Verification

- Ensure that the result of the execution of a cryptographic protocol accomplishes the **EXPECTATIONS** of protocol users.

11



Methods of Protocol Verification

- Formal methods
- Epistemic logics
- AI-based Testing tools
- Mathematical modeling tools

12



Cryptographic Protocol Analysis Language - Evaluation System (CPAL-ES)

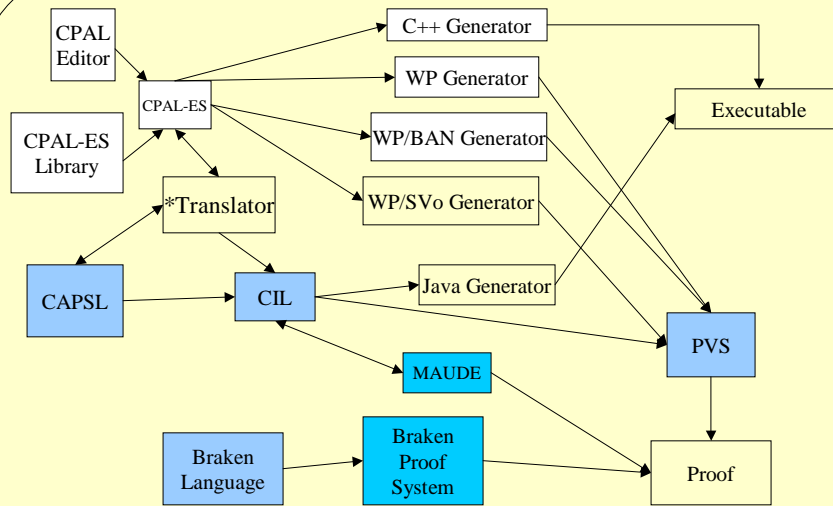
13



CPAL-ES

- Language for specifying security protocols
- Definition generator using Weakest Precondition reasoning
- Embedded simplification
- Connector to PVS for simplification
- Connector to BAN Logic

14



The CPAL Development Environment



Completed Projects

- CPAL Development Environment
– www.cs.fsu.edu/research/reports/TR-010502.pdf
- CPAL-ES Evaluation of the Transport Layer Security protocol
– www.cs.fsu.edu/research/reports/TR-000703.pdf



Ongoing Projects

- WTLS Analysis (Ilkay)
- Compare Athena & CPAL-ES (Ilkay)
- CPAL executable generator (Ravi)
- Wireless Protocols (Steve)

17



Open Projects

- Mathematical Formalism for Hashing
- Strategies for forming specifications for complex protocols (e.g. interleaving).
- Other logics integrated into CPAL-ES
- Expand the integration of CPAL-ES w/ PVS

18

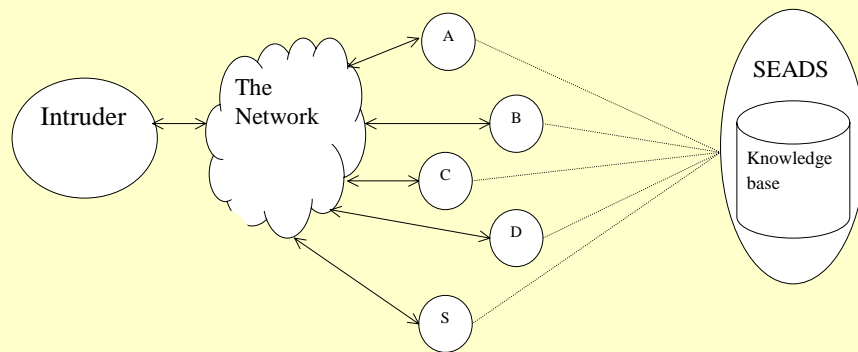


The Secure Enclave Attack Detection System (SEADS)

- Dynamic Analysis of Security Protocols
 - Learn about security protocol behavior from executing protocols
- Application Intrusion Detection for Secure Enclaves
 - Detect and prevent attacks on the fly



The Secure Enclave Attack Detection System





Intrusion Detection

- Detecting known attacks
 - Gather Signatures
 - Compare ongoing activity to the signatures
- Detecting abnormal behavior
 - Profiling
 - Compare ongoing activity to the profile

21



Protocol Knowledge Base Signatures

- The *essence* of a signature
 1. Session initiator & target IDs
 2. Protocol ID
 3. Message #
 4. Some combination of these
 5. Etc.

22



Needham/Schoreder Public Key Protocol

- 1. A -> B: $[n_a]PK_b$
- 2. B -> A: $[n_a, n_b]PK_a$
- 3. A -> B: $[n_b]PK_b$

- A -> M
- M_a -> B
- B -> A
- B -> A
- A -> M
- M_a -> B

- 1. A -> M: $[n_a]PK_m$
- 1'. M_a -> B: $[n_a, A]PK_b$
- 2'. B -> A: $[n_a, n_b]PK_a$
- 2. M -> A: $[n_a, n_b]PK_a$
- 3. A -> M: $[n_b]PK_m$
- 3'. M -> B: $[n_b]PK_b$

	Transition	Old State	New State
1	A -> M	Start	S ₁
2	A -> B	S ₁	S ₂
3	B -> A	S ₂	S ₃
4	M -> A	S ₃	S ₄
5	A -> M	S ₄	S ₅
6	A -> B	S ₆	Besson 23



Intrusion Detection Profiles

- Measurable behavior patterns
 1. # of session or public keys requested
 2. # of requests for your key
 3. # of failed or suspended sessions
 4. Etc.
- Measurement techniques



Completed Projects

- Papers:
 - New Security Paradigms Workshop, Sept 2000
 - ACM Workshop on Intrusion Detection Systems, Nov. 2000
- Projects
 - The Monitor, Alex Melendez, June 2001
 - www.cs.fsu.edu/research/reports/TR-010701.pdf
 - The Intrusion Detection Engine, Sachin Goregaker, August 2001
 - www.cs.fsu.edu/research/reports/TR-010703.pdf
 - The Knowledge Base, Nikhil Patel, Dec. 2001



Ongoing Projects

- B_SEADS Profile Handler (Leckie)
- B_SEADS Intrusion Detection Engine (Harley)
- AI Attack Recognizer (Yasinsac/McDuffie)



Practical Security

- Computer and Network Forensics
- Security Tools

27



Forensics Defined

- Methods and techniques for gathering evidence that can be used in court

28



Completed Projects

- Papers:
 - CNF, 2nd IEEE Systems, Man, and Cybernetics Information Assurance Workshop, USMA, June 2001
 - Honeytraps, submitted to 2002 International Symposium on Performance Evaluation of Computer and Telecommunication Systems

29



Security Tools

- Equipping SAIT Lab
 - Laboratory Environment
 - Tools Library

30



Completed Projects

- Security Laboratory Tools and Environment, Marion Bogdonav, Dec 2001
– www.cs.fsu.edu/research/reports/TR-011201.pdf

31



Other Interests

- Cryptography
- Models of Security

32



InfoSec Certificate

- Departmental Certificate
- NSA Approved
 - Only two universities in the world with NSA certification
- Details on the Departmental web page

33



Security and Assurance in Information Technology (SAIT) Laboratory

- Three separate laboratories
 - Network security
 - Cryptography
 - Virus
- Seeking corporate sponsorship
- Proposed Center of Excellence in Information Security

34



Funding Opportunities

- DoD Scholarships for Service
- Two grants proposals pending
- More to come

35



Closing Quotation

"I've had a wonderful time, but
this wasn't it."

- Groucho Marx (1895-1977)

36