

The background of the slide features several hand-drawn diagrams illustrating various security concepts:

- Buffer Overflow:** Diagrams showing memory addresses (e.g., 0x1E, 0x1D, 0x1C, 0x1B, 0x1A, 0x19, 0x18, 0x17, 0x16, 0x15, 0x14, 0x13, 0x12, 0x11, 0x10) and assembly-like instructions such as `pushl %ebp`, `movl %esp, %ebp`, and `subl $0a, %esp`. A buffer is shown overflowing with data, leading to a `DELAY` or `NOIS` state.
- Denial of Service (DoS):** Diagrams showing a `WEB SERVER` receiving a `REQ` (request) and a `RESP` (response). A `DELAY` is indicated, suggesting a service disruption.
- Cache Poisoning:** Diagrams showing a `SERVER` with a `MALICIOUS JAVASCRIPT CACHE` and a `CLIENT` (represented by a browser icon).
- Application Vulnerability:** Diagrams showing a `KDC` (Key Distribution Center) and various applications (`APP1`, `APP2`, `APP3`, `APP4`) interacting with a `SERVER`. A `REQ` is sent from the client to the server, and a `RESP` is returned.
- Code Snippets:** Several code snippets are scattered throughout, including `char* filename;`, `char buf[256];`, and `strcpy(buf, arg);`.

Conclusions

Fall 2011

Giovanni Vigna

University of California Santa Barbara

<http://www.cs.ucsb.edu/~vigna>

Topics Covered

- History, cryptography, and ethics
- Network vulnerability analysis (TCP/IP)
- Protocol vulnerability analysis (FTP, DNS)
- Application vulnerability analysis
- Web vulnerability analysis

From the Syllabus...

- This course focuses on how to analyze the security of a computer system
- This course will present concepts and approaches that allow one to design secure systems, evaluate their security posture, and detect/deflect attacks against them
- The course mixes a practical, hands-on approach with a discussion of the current research in the field
- Participants will learn how vulnerabilities are found and how these vulnerabilities can be exploited to compromise the security of a system
- This knowledge is a fundamental prerequisite for the correct design of protection systems

Giovanni Vigna, Advanced Topics in Security

Final Comment



With great power comes great responsibility

Giovanni Vigna, Advanced Topics in Security