

DNSSEC

Lecture 13

COMPSCI 726

Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

August 16, 2021

Source of some slides: **Princeton University, Cornell University,**
and **Stanford University**



DNSSEC



- Guarantees
 - Authenticity of DNS answer origin
 - Integrity of reply
- Accomplishes this by signing DNS replies
- Uses public key cryptography to sign responses
- Typically use trust anchors
 - Entries in the OS to bootstrap the process
- DNSSEC does not provide
 - Confidentiality

DNSSEC



- Cryptographically sign critical resource records
 - Resolver can verify the cryptographic signature

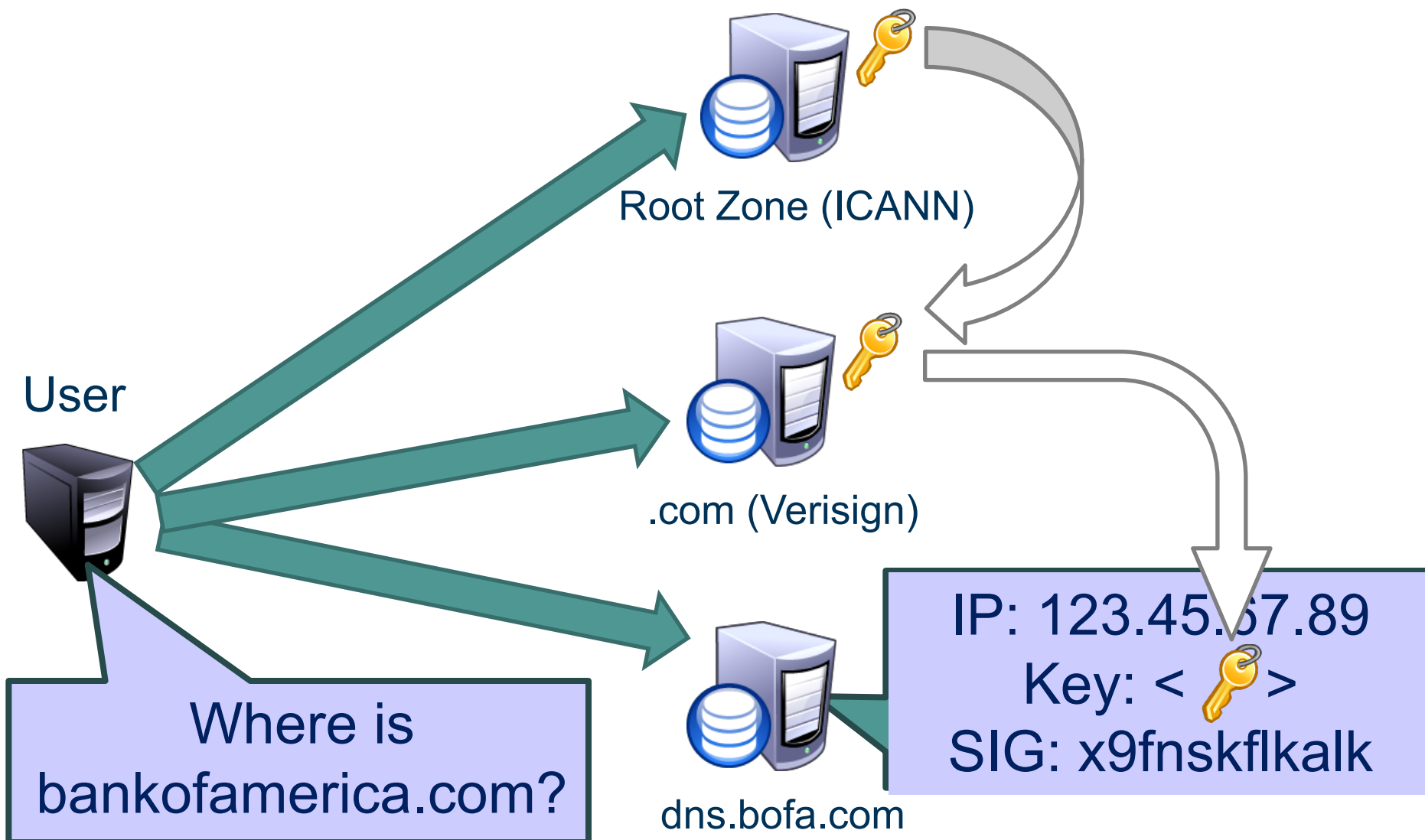
- Two new resource types
 - Type = DNSKEY
 - Name = Zone domain name
 - Value = Public key for the zone
 - Type = RRSIG
 - Name = (Type, name) tuple, i.e., the query itself
 - Value = Cryptographic signature on the query results

PURPOSE OF NEW RESOURCE TYPES

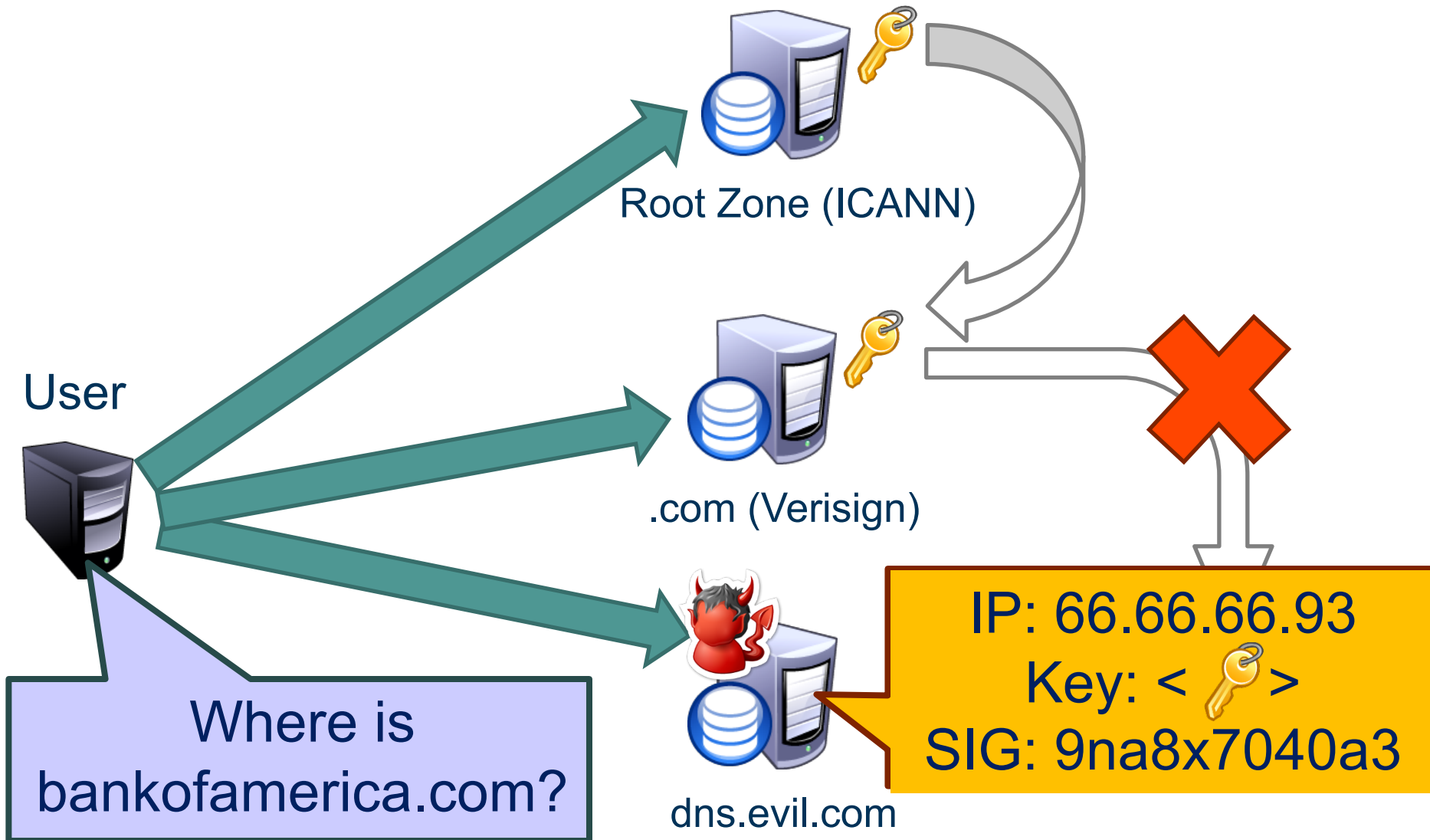


- DNSKEY
 - Creates a hierarchy of trust within each zone
- RRSIGN
 - Prevents hijacking and spoofing

DNSSEC HIERARCHY OF TRUST



DNSSEC HIERARCHY OF TRUST



DOES DNSSEC SOLVE ALL THE PROBLEMS?



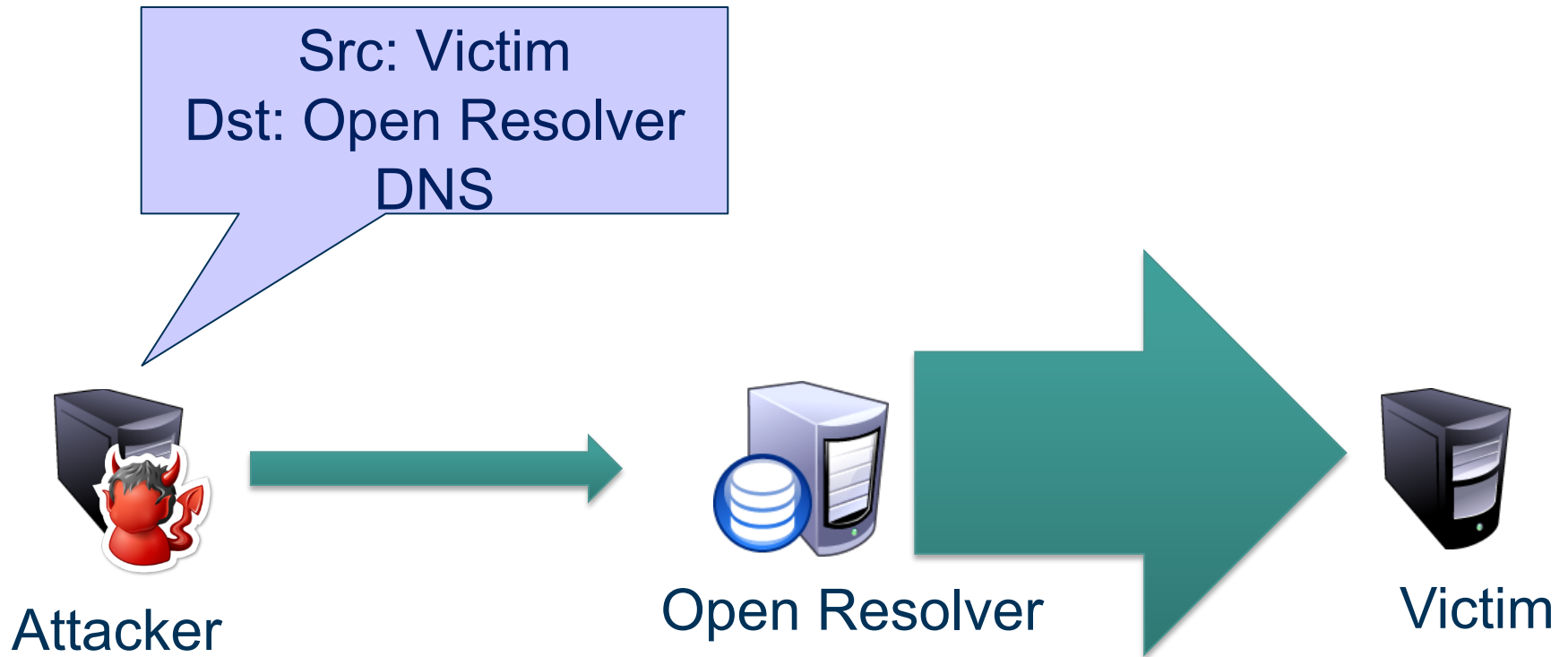
- No
- DNSSEC is vulnerable to
 - Amplification attack
 - Reflection attack

AMPLIFICATION ATTACK



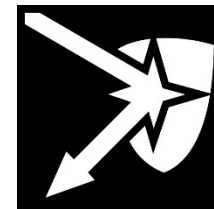
- Use packet(s) directed at a legitimate DNS
- Attacker creates DNS request(s) containing the spoofed source address of the target system
- Exploit DNS behaviour to convert a small request to a much larger response (amplification)
 - 60 bytes query → 512 bytes answer (~8.5x)
 - RFC 2671 allows larger DNS answers
 - Answers larger than 4000 bytes possible (>65x)
- Target is flooded with amplified responses

DNS AMPLIFICATION



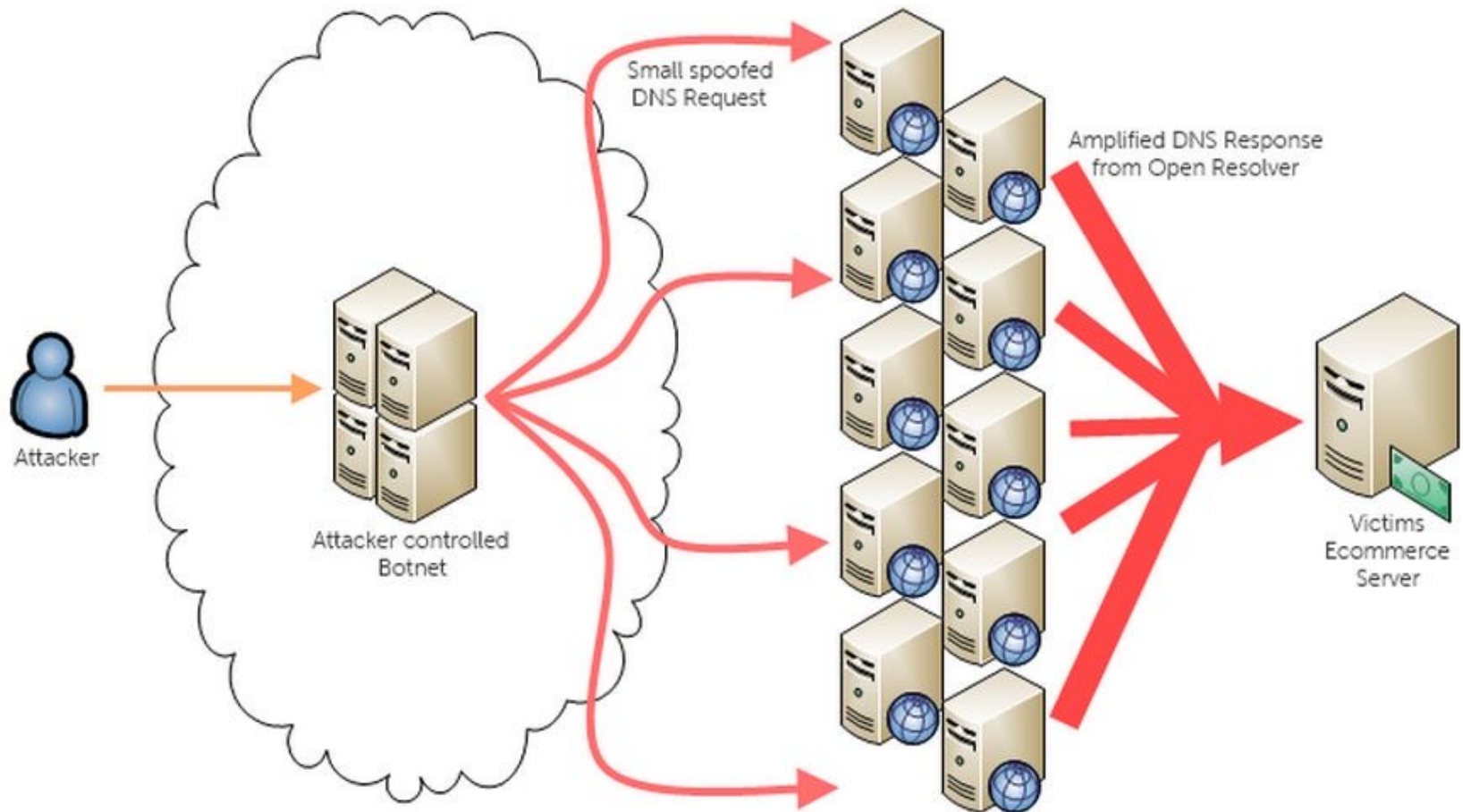
Sometimes, the DNS resolver network thinks it is under attack by the victim!

REFLECTION ATTACK



- Attacker sends packets to a known service with a spoofed source address of the actual target system
- The response is sent to the target
- “Reflects” the attack (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system

REFLECTION ATTACK – DDOS



SOME COUNTERMEASURES



- Check your network is configured to prevent spoofed traffic from leaving your network
- Make sure that your name servers are not answering recursive queries for random domains for random users

SUMMARY



- DNSSEC guarantees authenticity and integrity
- DNSSEC does not provide confidentiality
- DNSSEC is vulnerable to DDoS
- There are general countermeasures
 - Check traffic leaving your network
 - Do not answer recursive queries

RESOURCES



- Arends, Roy, Rob Austein, Matt Larson, Dan Massey, and Scott Rose. **DNS Security Introduction and Requirements**. RFC 4033, 2005.
Available at: <https://tools.ietf.org/html/rfc4033>
- **The Continued Rise of DDoS Attacks.**
Available at:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf



Questions?

Thanks for your attention!