Mecanismos de Segurança aplicados a Interface para o Sistema de Roteamento (I2RS)

Joel Molling[1], **Jeferson Campos Nobre**[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
CEP 93.022-000 – São Leopoldo – RS – Brasil

Abstract. *The frequent security incidents related to infrastructure networks and the Internet, emphasize the importance of management mechanisms to apply security controls to the network elements. The proposed project presents the evaluation of a model based on I2RS, which aims to add security to the process management and configuration of existing routing infrastructure of a computer network.*

Resumo. *Os constantes incidentes de segurança relacionados a infraestrutura de redes e à Internet, ressaltam a importância de mecanismos de gerenciamento que permitam aplicar controles de segurança aos elementos de rede. O trabalho proposto apresenta a avaliação de um modelo baseado em I2RS, que visa agregar segurança no processo de gerenciamento e configuração das atuais infraestruturas de roteamento de uma rede de computadores.*

1. Introdução

O advento da Internet facilitou à expansão dos negócios e possibilitou às organizações proverem interoperabilidade às suas operações. A necessidade de manter um ambiente de interconexão de rede estável, demonstrou o quão importantes e imprescindíveis são os mecanismos de administração em uma rede de computadores.As tecnologias de administração deveriam possibilitar a gestão, o controle e a manutenção dos dispositivos presentes no ambiente de rede, sem que houvessem impactos na operação e consequentemente as atividades de uma organização. Para [Shin et al. 2012], a administração de uma rede já se tornava uma tarefa complexa e crítica, uma vez que as tecnologias de rede já não suportavam mais a constante evolução da infraestrutura de redes de computadores.

As tecnologias existentes não proporcionavam uma gestão centralizada do ambiente, permitindo que ameaças pudessem comprometer a rede sem uma imediata identificação e correção dos problemas. A complexidade da análise necessária para solucionar os problemas, era proporcional ao tamanho da rede. Os problemas quando relacionados a infraestrutura de roteamento da rede, eram ainda mais difíceis de se identificar, uma vez que protocolos como RIP (*Routing Information Protocol*), EIGRP (*Enhanced Interior Gateway Routing Protocol*) e OSPF (*Open Shortest Path First*), não eram providos de grandes mecanismos de segurança, aumentando o vetor de ataque.

O novo paradigma de Redes Definidas por Software (*Software-Defined Networking* – SDN), permitiu através do conceito de abstração dos elementos de rede, a gestão e o controle do ambiente de forma centralizada [Drutskoy et al. 2013]. Segundo [McKeown et al. 2008], SDN ao contrário do modelo tradicional, proporciona uma maior flexibilidade às tarefas de administração de uma rede, possibilitando análises e correções mais eficazes.

SDN sendo flexível, possibilitou um ambiente para o desenvolvimento de novas tecnologias que pudessem aprimorar e também agregar novas funcionalidades ao conceito de redes programáveis. Uma dessas tecnologias, a Interface para o Sistema de Roteamento (*Interface to the Routing System* - I2RS), trouxe como premissa o desenvolvimento de uma camada que possibilitasse o devido controle e gerenciamento da infraestrutura de roteamento da rede. O I2RS incorporou ao conceito de SDN, agilidade e eficiência na manipulação dos protocolos e regras de roteamento que mantém uma rede [Hares and White 2013].

A camada de gerenciamento criada pelo I2RS, por mais que forneça características como a análise de comportamento dos protocolos, até o presente momento não é capaz de proporcionar segurança às tarefas de administração da infraestrutura de roteamento, visto que muitas vulnerabilidades estão localizadas diretamente na estrutura ou no comportamento individual dos protocolos. Como alternativa para solucionar os problemas de segurança do I2RS, é proposta a utilização do protocolo de configuração de redes (*Network Configuration Protocol* - NETCONF), em conjunto com a linguagem de modelação de dados YANG. O NETCONF/YANG no contexto I2RS, tem a função de transportar as requisições I2RS na rede, fornecer segurança para a comunicação entre cliente e agentes I2RS, e prover segurança ao armazenamento das informações nos elementos da rede [Haas 2015].

O trabalho se propõe a avaliar o modelo NETCONF/YANG como sendo o mecanismo de segurança definido pelo I2RS e objetiva compará-lo aos mecanismos de segurança providos pelos atuais protocolos de roteamento.

2. Interface para o Sistema de Roteamento

[Hu et al. 2014], descrevem o conceito de arquitetura SDN como não sendo algo inovador por completo, fazendo referência a computação em nuvem que já possibilitava a abstração do sistema operacional das intensas instruções de hardware. A separação que SDN proporciona ao universo de redes de computadores, possibilita um ganho de desempenho no quesito de gerenciamento, controle e manipulação dos dados trafegados entre as redes [Hu et al. 2014]. Com SDN é possível controlar o fluxo de dados, gerenciar políticas de segurança e prioridades de tráfego através de um ponto único de controle, sem a necessidade de configuração individual de cada equipamento [ONF 2012].

Para [Hu et al. 2014], as características de SDN ficam evidenciadas quando é feito um comparativo com as tradicionais redes de computadores. Entre as principais características e vantagens em comparação ao modelo atual, é possível destacar a inteligência e velocidade, que torna mais eficiente o uso dos recursos, otimizando a distribuição de carga e dando mais agilidade as transmissões [Hu et al. 2014]. SDN proporciona facilidade no gerenciamento da rede, pois com a utilização de um ponto central para gerenciamento dos dispositivos de comutação, permite agilidade e eficiência às tarefas de configuração [Shin et al. 2012].

Entre as diversas arquiteturas existentes para a elaboração de um modelo de SDN, o *Internet Research Task Force* (IRTF), através de um de seus grupos de pesquisa denominado de *Software-Defined Networking Research Group* (SDNRG), definiu uma arquitetura de SDN. O modelo definido é devidamente abordado na RFC 7149, que descreve o conceito de separação entre os planos de controle e de dados.

A arquitetura de SDN possui as funções de gerenciamento de rede acopladas a camada de controle (*Control Layer*), que baseada em Software possibilita a sua programação conforme necessário, dando origem ao nome SDN. Essa arquitetura faz também com que a camada de aplicação (*Application Layer*) interprete a rede como sendo algo único [ONF 2012]. O conceito de redes programáveis delegou aos administradores da rede um poder de gerenciar, configurar e proteger a rede através de automatizações aplicadas à camada de controle. A arquitetura SDN permite ainda a implementação de *Application Program Interfaces* (APIs), que possibilitam a inclusão de serviços de rede como engenharia de tráfego, qualidade de serviço, controle de acesso e segurança [ONF 2012]. Entre as APIs de SDN, destacam-se duas: as interfaces sul (*SouthBound*) e norte (*NorthBound*).

Segundo [Kreutz et al. 2015], *NorthBounds* são as APIs que fornecem uma interface para o desenvolvimento de aplicações e as responsáveis por abstrair as instruções utilizadas pelas interfaces sul. Essas instruções consumidas pelas *SouthBounds*, são necessárias para programar e configurar os dispositivos presentes na camada de infraestrutura [Kreutz et al. 2015].

Southbounds são interfaces que buscam facilitar e tornar mais eficiente o controle da rede, permitindo que o controlador faça alterações dinâmicas de acordo com a necessidade e da forma mais ágil possível. Segundo [Kreutz et al. 2015], as interfaces sul são responsáveis por definir os protocolos de comunicação entre os dispositivos de encaminhamento de tráfego e o plano de controle. Soluções conhecidas como *southbounds* abertos, são o OpenFlow, o *Simple Network Management Protocol* (SNMP) e o NETCONF. O Openflow através de seu controlador, propõe uma administração centralizada dos dispositivos de rede, permitindo controle e manipulação sobre o fluxo dos dados trafegados entre a rede [Rothenberg et al. 2010]. A característica de utilizar o conceito de fluxo, apesar de altamente eficaz, não exerce funções de administração sobre a estrutura de roteamento da rede, permitindo uma distinção entre OpenFlow e I2RS, que oferece uma camada de gerenciamento de mais alto nível, operando em conjunto com os protocolos de roteamento [FUGITSU 2014].

O I2RS, projeto de um grupo de trabalho[1] do *Internet Engineering Task Force* (IETF), foi criado com o propósito de viabilizar soluções para o atual sistema de roteamento das redes de computadores sobre o conceito de SDN. Entre os objetivos, estão a elaboração de uma arquitetura de alto nível para o I2RS, incluindo gerenciamento de políticas de roteamento e segurança, e análise do funcionamento de protocolos de roteamento, aprimorando gerenciamento e desempenho.

A arquitetura do I2RS é composta por um cliente e um agente, sendo o primeiro, responsável pelo gerenciamento e dispersão das regras através do canal de comunicação estabelecido. Os agentes, localizados no elemento de rede, são responsáveis por aplicar as requisições encaminhadas pelos clientes. De acordo com o *Internet Draft* proposto por [Hares and White 2013], é possível estruturar uma arquitetura de um ou mais agentes I2RS. Em arquiteturas simples onde há somente um cliente, todo o gerenciamento é centralizado, ao contrário de arquiteturas mais robustas que incluem múltiplos clientes I2RS, cada qual com uma função específica e ambos operando em conjunto com os diversos agentes remotos.

[1] http://datatracker.ietf.org/wg/i2rs

2.1. Gerenciamento do Sistema de Roteamento

Segundo [Haas 2015], para alcançar os objetivos propostos pelo projeto, era necessário que o I2RS pudesse estabelecer uma infraestrutura capaz de manipular o estado de configuração dos elementos da rede, provendo uma interface segura e capaz de controlar a estrutura de roteamento de uma rede. Para possibilitar o transporte das requisições I2RS e atender aos requisitos de segurança, como autenticação mútua, controle de acesso a estrutura de dados de cada dispositivo, confidencialidade e integridade das informações, o grupo de trabalho de I2RS do IETF definiu o NETCONF como mecanismos de suporte às funções de transporte, segurança e configuração necessárias para a implementação do I2RS. O NETCONF é um protocolo de gerenciamento de rede, mantido pelo IETF e publicado sobre a RFC 4741. Segundo [Wallin and Wikström 2011], o NETCONF provê mecanismos que permitem a instalação, exclusão e manipulação de configuração em dispositivos de rede enquanto estão em operação, através da utilização do conceito de armazenamento lógico.

[Choi et al. 2004] apresenta que o conceito de armazenamento lógico do NETCONF utiliza uma codificação de dados baseada em XML, onde todas ações são realizadas através de chamadas de procedimento remoto (*Remote Procedure Call* - RPC), que permitem a comunicação entre gerente e agente NETCONF. As chamadas RPC podem ser estabelecidas por protocolos como BEEP (*Blocks Extensible Exchange Protocol*), SSH (*Secure Shell Transport*), SSL (*Secure Sockets Layer*), TLS (*Transport Layer Security*) e SOAP (*Simple Object Access Protocol*) [Huang et al. 2009]. Segundo [Schonwalder et al. 2010], a camada RPC sobre a estrutura de protocolos de transporte são a base funcional do NETCONF, com o nível de manipulação e estruturação dos dados ocorrendo na camada de operação da arquitetura do NETCONF.

A camada mais inferior da arquitetura, denominada de camada de transporte seguro, nativamente utiliza o protocolo SSH para transporte de suas mensagens, que o torna muito semelhante as interfaces de linha de comando (Command Line Interfaces - CLI) proprietárias, que por sua vez são embarcadas aos dispositivos [Wallin and Wikström 2011]. O transporte através de SSH é o responsável pelo NETCONF atender a três importantes quesitos de segurança, como confidencialidade e integridade das informações, além da existência de um processo de autenticação.

A estrutura de armazenamento lógico, definida com o uso de NETCONF, é parte fundamental para implementação do I2RS, uma vez que é possível trabalhar com mecanismos de injeção de configuração em bases efêmeras ou não efêmeras, no caso do NETCONF, uma base *writable-running* ou *writable-running + startup*. O processo de injeção de configuração, além de permitir a utilização do conceito de bases de dados efêmeras, designou a linguagem de modelação de dados YANG como padrão de estrutura para as informações que são enviadas aos dispositivos com NETCONF e gerenciados pelo I2RS. A definição do YANG também é fundamental para garantir a confiabilidade das informações I2RS, principalmente quanto ao controle de acesso às informações armazenadas nos dispositivos.

O YANG, uma linguagem de modelação de dados padronizada e definida pelo IETF, revela uma abordagem distinta dos modelos XML atuais. [Schonwalder et al. 2010], retratam que o objetivo do YANG é ser uma linguagem legível e de alta compreensão para modelar os dados NETCONF. Segundo [Xu and Xiao 2008],

Tabela 1. Protocolos sem mecanismos de segurança x Ameaças

Protocolos / Ameaças	Eavesdropping	Personificação	Spoofing	Null Session	Session Hijack	Replay	Denial of Service
RIP	V	V	V	V	V	V	V
RIPv2	V	V	V		V	V	V
EIGRP	V	V	V		V	V	V
OSPF	V	V	C		V	V	V

V=Vulnerável; C=Combinação;

o formato de linguagem XML foi introduzido ao protocolo de configuração de redes para padronizar a linguagem responsável por modelar os dados. Embora já existam esquemas XML como XSD e RelaxNG em utilização junto ao NETCONF, ambos possuem características que dificultam a compreensão da linguagem, principalmente quando grande parte das extensões do protocolo são utilizadas, criando a necessidade de utilização do YANG [Schonwalder et al. 2010].

[Xu and Xiao 2008] em sua pesquisa, fazem um comparativo entre um Schema XML, YANG e SMI. Nesse estudo, [Xu and Xiao 2008] apresentam o quanto a linguagem YANG pode ser superior aos tradicionais métodos XML empregados com o NETCONF. Entre as questões abordadas, o YANG é amplamente superior no quesito segurança, prezando por conceitos como confidencialidade e integridade dos dados, além de possuir mecanismos de controle de acesso e bloqueio às informações.

3. Trabalho Proposto - Avaliação

O objetivo da avaliação apresentada nesta Seção é efetuar um comparativo entre os mecanismos de segurança atualmente aplicados aos protocolos de roteamento e as soluções de segurança providas pelo modelo de gerenciamento e controle proposto pelo I2RS, que atua em conjunto com o protocolo NETCONF e a linguagem de modelação de dados YANG. Apresenta-se uma análise qualitativa que demonstra a quais ameaças os protocolos de roteamento e o NETCONF estão vulneráveis.

3.1. Mecanismos de Segurança x Ataques

A avaliação consiste em uma análise qualitativa que apresenta os resultados de uma comparação entre os protocolos de roteamento e ataques aos quais estão vulneráveis. Primeiramente, a Tabela 1 demonstra a quais ataques estão suscetíveis os protocolos de roteamento quando não há ou não estão ativos os mecanismos de segurança.

O protocolo RIP em sua versão 1 não possui mecanismos de segurança agregados a sua estrutura, o que permite que ataques como *Spoofing* e *Replay* possam explorar vulnerabilidades do protocolo e obter vantagens sobre a sua estrutura e implementação. Apesar da versão 2 do RIP já possuir uma estrutura mais robusta, contendo mecanismos de segurança, ela continua sendo vulnerável a ataques maliciosos caso os mecanismos de segurança não sejam ativados pelos administradores do ambiente. O EIGRP com a característica de ser um protocolo híbrido e tendo o seu funcionamento baseado em um algoritmo muito semelhante ao utilizado pelo RIP, está sujeito as mesmas ameaças.

O protocolo OSPF é baseado no algoritmo de menor rota primeiro (*Shortest Path First* - SPF), que diferente dos protocolos anteriormente citados, foi projetado com uma infraestrutura mais robusta a qual nativamente já aplica alguns controles de segurança.

Tabela 2. Protocolos com mecanismos de segurança x Ameaças

Protocolos / Ameaças	Eavesdropping	Personificação	Spoofing	Null Session	Session Hijack	Replay	Denial of Service
RIP	V	V	V	V	V	V	V
RIPv2	V	V	V		V	V	V
S-RIP			C				V
EIGRP	V	V	V		V	V	V
OSPFv2	V	V	C		V	V	V
Digital Signature OSPF			C				
NETCONF over SSH							
NETCONF over TLS							

V=Vulnerável; C=Combinação;

Entre os mecanismos são aplicados controles aos números de sequência das mensagens de atualização e idade dos pacotes, o que inibe diretamente ataques de *Spoofing*. O mecanismo atribuído aos pacotes LSA não evita por completo tentativas de *Spoofing*, mas torna-as possíveis somente em casos de combinação, onde o atacante primeiro compromete algum roteador através de outro ataque para então utilizá-lo como recurso para uma nova ação.

A Tabela 2 ilustra que o cenário de ameaças é completamente diferente quando os mecanismos de segurança são devidamente aplicados ao ambiente, reduzindo o vetor de ataques e possibilitando mais segurança à infraestrutura de rede.

Os mecanismos de segurança incorporados a estrutura dos protocolos RIPv2, EIGRP e OSPFv2, se resumem a utilização da função de hash MD5 durante o processo de autenticação dos dispositivos adjacentes. Apesar dessa função criptográfica prover segurança na troca de informações, garantindo a verificação de autenticidade e integridade das mensagens, o MD5 só inibe ataques como *Spoofing*, *Session Hijack* e personificação, quando estes são executados diretamente à estrutura de roteamento, sem a combinação ou intervenção de outro ataque. O problema de não evitar ataques combinados, compromete a segurança de toda a rede caso um atacante consiga explorar uma vulnerabilidade de configuração de um dispositivo, permitindo acesso irrestrito ao mesmo e a rede por completo.

A função MD5, apesar de ainda ser utilizada em larga escala, não é mais recomendada para novas implementações, visto que a técnica de hash aplicada no MD5 já é criptograficamente insegura e passível de colisão, uma técnica que busca encontrar dois conjuntos de dados com o mesmo hash [Kuznetsov 2014]. [Wang et al. 2004] demonstra colisões de MD5 em seu primeiro trabalho e posteriormente apresenta dois certificados digitais com o mesmo hash MD5 [Lenstra et al. 2005].

O S-RIP, uma extensão do protocolo RIP, foi proposto por [Wan et al. 2004] para maximizar a segurança e reduzir o vetor de ataques sobre os protocolos que utilizam o algoritmo de vetor de distância. Os autores apresentam uma proposta de segurança que tem como objetivos a prevenção de ataques de personificação, espionagem e roubo de sessão. Em sua abordagem, [Wan et al. 2004] utilizam chaves compartilhadas distintas para cada par de roteadores adjacentes, o que aumenta a complexidade do ambiente e dificulta o sucesso do atacante, mesmo com o processo de autenticação sendo feito através de MD5. Para o controle de ataques como *Spoofing*, espionagem e roubos de sessão, o

S-RIP trabalha com um mecanismo que avalia a consistência dos pacotes através de testes de aproximação.

[Murphy and Badger 1996] apresentam uma proposta de melhorar o protocolo OSPF através da implementação de mecanismos de segurança baseados em criptografia assimétrica, especialmente com a utilização do conceito de assinatura digital (*Digital Signature*). O *Digital Signature OSPF* aumenta a força do processo de autenticação entre os dispositivos da infraestrutura de roteamento, provendo um ambiente seguro às trocas de mensagens do protocolo e inibindo ataques antes possíveis contra a função de hash MD5. Apesar de possuir um mecanismo forte de segurança, o *Digital Signature OSPF* não evita ataques de *Spoofing* pois geralmente são iniciados de dentro da rede e através de um dispositivo comprometido, burlando a segurança do processo assimétrico.

4. Considerações Parciais

A escolha do projeto I2RS pelo NETCONF, apesar de obter ganhos de gerenciamento, também é relacionada as técnicas de segurança que o mesmo agrega ao modelo proposto. O NETCONF trabalhando sobre SSH, proporciona segurança a níveis de autenticação, integridade e confidencialidade, superando em qualidade a segurança dos protocolos de roteamento durante o transporte das mensagens pela infraestrutura de rede. O ganho de segurança com NETCONF permite uma eficácia na proteção à ameaças dos mais variados aspectos de ataque, inclusive ataques de negação de serviço. A proteção contra DoS é possível devido a união das características do I2RS, que identifica alterações e comportamentos anômalos na topologia de rede, com os recursos fornecidos pelo NETCONF, que através de uma comunicação extremamente ágil, possibilita injeções de configuração do cliente I2RS nos agentes remotos até mesmo durante a execução de um ataque.

Nesse momento, objetiva-se avaliar de forma experimental e em laboratório os cenários existentes, a fim de medir de forma quantitativa os ganhos de desempenho e gerenciamento que o modelo NETCONF/YANG/I2RS possibilita.

Referências

[Choi et al. 2004] Choi, M.-J., Choi, H.-M., Hong, J., and Ju, H.-T. (2004). Xml-based configuration management for ip network devices. *Communications Magazine, IEEE*, 42(7):84–91.

[Drutskoy et al. 2013] Drutskoy, D., Keller, E., and Rexford, J. (2013). Scalable network virtualization in software-defined networks. *Internet Computing, IEEE*, 17(2):20–27.

[FUGITSU 2014] FUGITSU (2014). Technical report - carrier software defined networking (sdn). Disponível em: <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/SDN$_{R}eport.pdf$¿.

[Haas 2015] Haas, J. (2015). I2rs requirements for netmod/netconf. Internet-Draft draft-haas-i2rs-netmod-netconf-requirements-01, IETF Secretariat. `http://www.ietf.org/internet-drafts/draft-haas-i2rs-netmod-netconf-requirements-01.txt`.

[Hares and White 2013] Hares, S. and White, R. (2013). Software-defined networks and the interface to the routing system (i2rs). *Internet Computing, IEEE*, 17(4):84–88.

[Hu et al. 2014] Hu, F., Hao, Q., and Bao, K. (2014). A survey on software-defined network and openflow: From concept to implementation. *Communications Surveys Tutorials, IEEE*, 16(4):2181–2206.

[Huang et al. 2009] Huang, J., Zhang, B., Li, G., Gao, X., and Li, Y. (2009). Challenges to the new network management protocol: Netconf. In *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*, volume 1, pages 832–836.

[Kreutz et al. 2015] Kreutz, D., Ramos, F., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., and Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76.

[Kuznetsov 2014] Kuznetsov, A. (2014). An algorithm for md5 single-block collision attack using high-performance computing cluster.

[Lenstra et al. 2005] Lenstra, A., Wang, X., and de Weger, B. (2005). Colliding x.509 certificates. Cryptology ePrint Archive, Report 2005/067. `http://eprint.iacr.org/`.

[McKeown et al. 2008] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74.

[Murphy and Badger 1996] Murphy, S. and Badger, M. (1996). Digital signature protection of the ospf routing protocol. In *Network and Distributed System Security, 1996., Proceedings of the Symposium on*, pages 93–102.

[ONF 2012] ONF (2012). Software-defined networking - the new norm for networks. Disponível em: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[Rothenberg et al. 2010] Rothenberg, C., Nascimento, M., Salvador, M., and Magalhães, M. (2010). Openflow e redes definidas por software: um novo paradigma de controle e inovação em redes de pacotes. *Cad. CPqD Tecnologia,*, 7(1):65–76.

[Schonwalder et al. 2010] Schonwalder, J., Bjorklund, M., and Shafer, P. (2010). Network configuration management using netconf and yang. *Communications Magazine, IEEE*, 48(9):166–173.

[Shin et al. 2012] Shin, M.-K., Nam, K.-H., and Kim, H.-J. (2012). Software-defined networking (sdn): A reference architecture and open apis. In *ICT Convergence (ICTC), 2012 International Conference on*, pages 360–361.

[Wallin and Wikström 2011] Wallin, S. and Wikström, C. (2011). Automating network and service configuration using netconf and yang. In *Proceedings of the 25th International Conference on Large Installation System Administration*, LISA'11, pages 22–22, Berkeley, CA, USA. USENIX Association.

[Wan et al. 2004] Wan, T., Kranakis, E., and van Oorschot, P. (2004). S-rip: A secure distance vector routing protocol. In Jakobsson, M., Yung, M., and Zhou, J., editors, *Applied Cryptography and Network Security*, volume 3089 of *Lecture Notes in Computer Science*, pages 103–119. Springer Berlin Heidelberg.

[Wang et al. 2004] Wang, X., Feng, D., Lai, X., and Yu, H. (2004). Collisions for hash functions md4, md5, haval-128 and ripemd. Cryptology ePrint Archive, Report 2004/199. `http://eprint.iacr.org/`.

[Xu and Xiao 2008] Xu, H. and Xiao, D. (2008). Data modeling for netconf-based network management: Xml schema or yang. In *Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on*, pages 561–564.