

সামাজিক নিরাপত্তা: সিকিউরিটিজের বিভিন্ন স্তর

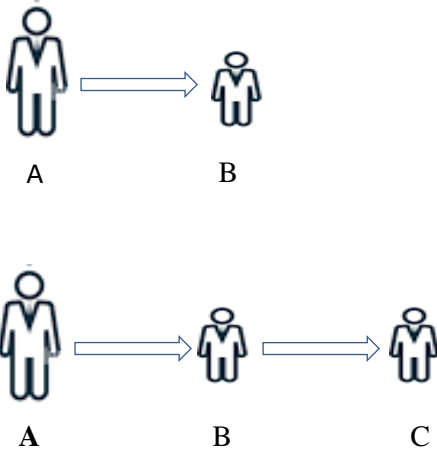
দুলাল আচার্য
পরিচালক ও অধ্যাপক
ফলিত কম্পিউটার প্রযুক্তি, কলকাতা, ভারত।
ইমেইল: dulal@actsoft.org

ভূমিকা:

সামাজিক নিরাপত্তা প্রদান একটি এলাকার প্রতিবেশীদের জন্য ব্যবস্থা এবং সতর্কতা নির্ধারণের ধারণা। যখন বিভিন্ন স্তর থেকে বিপদ আসে এবং যে কোনও এলাকায় ক্ষয়ক্ষতি হয়, তখন অপরাধীদের উত্স খুঁজে বের করা খুব কঠিন। কিছু আক্রমণ আছে যা শীর্ষ স্তর থেকে আসে এবং অনেক স্তর অতিক্রম করার পরে এটি অবশেষে লক্ষ্যে কার্যকর হয়। এই লেখায় মাল্টি লেভেল ভিত্তিক আক্রমণের কিছু ধারণা, সংশ্লিষ্ট সতর্কতা, অনুপ্রবেশকারীদের দ্বারা ভাড়া করা দুর্নীতিগ্রস্ত সংস্থানগুলিকে বিপদমুক্ত করা এবং মাল্টি লেভেল ভিত্তিক আক্রমণ সম্পর্কে সচেতনতা গড়ে তোলার বিষয়ে আলোচনা করা হয়েছে।

মাল্টি লেভেল আক্রমণ কি?

আক্রমণকারী যখন সরাসরি কোনো ক্ষতি করে না কিন্তু মূল পরিকল্পনাকারীকে লুকানোর জন্য বিভিন্ন স্তরের লোকের (বা সংস্থান) সাহায্য নেয় তাকে মাল্টি লেভেল অ্যাটাক বলে। ধরুন, 'A' 'C' অঞ্চলের মধ্যে একজন ব্যক্তিকে হত্যা করার পরিকল্পনা করেছে, তাই, 'A' 'B' অঞ্চলের এক বা একাধিক ব্যক্তিকে নিয়োগ করবে এবং 'B' পরিকল্পনা কার্যকর করার জন্য 'C'-এর কাছে প্রয়োজনীয় তথ্য পাঠাবে। একটি চিত্রের সাহায্যে ধারণাটি ব্যাখ্যা করা হয়েছে:



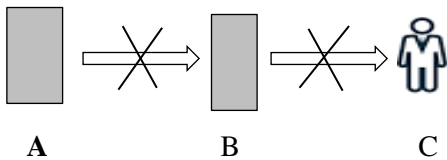
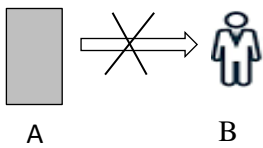
চিত্র-১: (ক) নেটওয়ার্কের দুই স্তর এবং (খ) আক্রমণকারীদের দ্বারা সাজানো নেটওয়ার্কের তিন স্তর।

উপরের চিত্র 1(ক), 'A' পরিকল্পনাকারী এবং 'B' নির্বাহক হিসাবে পরিচিত। চিত্র 1(খ) তিনজনের মধ্যে, 'A' হল পরিকল্পনাকারী, 'B' হল ভাড়া করা ব্যক্তি এবং একজন উপ-পরিকল্পক, 'C' হল নির্বাহক। উভয়

ক্ষেত্রেই, 'C' হল নির্বাহক এবং হতে পারে একজন ব্যক্তি বা একটি স্বয়ংক্রিয় সিস্টেম যেমন; বোমা ফাটানো রিমোট সার্কিট, স্বয়ংক্রিয় ফায়ারিং ডিভাইস, টাইমার সহ গাড়ি বোমা বা সময় এবং আবহাওয়া ইত্যাদির সাথে সংক্রামিত যেকোন জৈবিক অস্ত্র, কারণ, অ্যাকশনের পরে, 'C' সম্পূর্ণরূপে ক্ষতিগ্রস্ত এবং ছড়িয়ে ছিটিয়ে আছে- যেখানে ফরেনসিক তদন্ত অনুসন্ধানের কারণ খুঁজে পেতে পারে, কিন্তু 'B' এবং 'A'-এর নেটওয়ার্ক লিঙ্ক খুঁজে বের করা সবচেয়ে কঠিন কাজ।

B-এর বৈশিষ্ট্য: তাকে নিয়োগ দেওয়া হয় বা প্রশিক্ষিত করা হয় এবং কিছু আক্রমণ করতে উদ্বুদ্ধ করা হয়। যদি 'B' অর্থগ্রহণকারী ব্যক্তি হয়, তবে সে ক্ষতি বা বিস্ফোরণের প্রমাণ সংগ্রহের জন্য অপেক্ষা করবে যা তার বাকি অর্থ গ্রহণ নিশ্চিত করবে। যদি 'B' কোনো রাজনৈতিক দলের সদস্য হয় বা রাজনৈতিকভাবে উদ্বুদ্ধ কোনো সন্ত্রাসী সংগঠনের সদস্য হয়, তাহলে সে ক্ষতির প্রমাণ সংগ্রহের জন্য অপেক্ষা করবে না। তিনি টিভি, রেডিও, কাগজের খবর ইত্যাদির মতো অন্যান্য উত্স থেকে তথ্য সংগ্রহ করবেন। সবচেয়ে বুদ্ধিমান নেটওয়ার্ক ডিজাইনিং 'B' এর উপর নির্ভর করে, যদি 'B' একজন উদ্বৃত্ত মানুষ বা ঘোরাফেরাকারী ব্যক্তি হয়- যে সময়ে সময়ে তার অবস্থান পরিবর্তন করে, তাহলে, তদন্ত, উদাহরণস্বরূপ- বিস্ফোরণ, সবচেয়ে কঠিন হয়ে ওঠে।

ডিলিংকিং নেটওয়ার্ক: চিত্র-2.(ক) এ, A-B হিসাবে একটি লিঙ্ক রয়েছে; যদি যোগাযোগ প্রযুক্তির ধারণা থেকে চিন্তা করা হয়, A এবং B এর মধ্যে যোগাযোগের দুটি চ্যানেল রয়েছে এবং এগুলি হল A-B এবং B-A আপলিংক এবং ডাউনলিংক নামে পরিচিত। এর অর্থ হল, আক্রমণের আগে, উভয় চ্যানেলই আক্রমণ কার্যকর করার পরিকল্পনা করার জন্য সক্রিয় থাকে, কিন্তু, কার্যকর করার পরে, আক্রমণকারীদের উত্স সম্পর্কে তথ্য গোপন করার জন্য উভয় চ্যানেল বা একটি চ্যানেলের সংযোগ বিচ্ছিন্ন বা ধ্বংস করা হয়। চিত্র-2.(খ) এ, দুটি লিঙ্ক A-B এবং B-C রয়েছে, মনে করা হয় যে A-C-এর মধ্যে কোনো যোগাযোগ নেই কারণ, 'A' 'C'-এর সাহায্যে কার্যকর করার জন্য 'B'কে নিয়োগ করেছে। এই নেটওয়ার্কে 'A' নিজেকে লুকিয়ে রাখতে চায়। যখন সমস্ত পরিকল্পনা এবং বাস্তবায়নের অধিকার 'C'-এর কাছে হস্তান্তর করা হয়, তখন 'B' লিঙ্ক 'B-C'কে ডিলিঙ্ক করতে পারে এবং A, 'A-B' লিঙ্ককে ডিলিঙ্ক করতে পারে অথবা নীচে দেখানো হিসাবে তারা আপ এবং ডাউন উভয় চ্যানেল ডিলিঙ্ক করতে পারে।



চিত্র 2. (ক) আক্রমণ শেষ হওয়ার পরে A অদৃশ্য হয়ে যায় এবং A-B এর সংযোগ বিচ্ছিন্ন হয়ে যায়। (খ) A এবং B লুকানোর এবং A-B এবং B-C এর সংযোগ বিচ্ছিন্ন করার একটি মডেল দেখানো দেখানো হয়েছে।

তথ্য সংগ্রহ:

সন্দেহভাজন ব্যক্তি বা ঘটনা সম্পর্কে তথ্য সংগ্রহ করা একটি আইনি কাজ। আমরা কি কোনো ব্যক্তি বা এলাকার কম্পিউটারের সার্ভারে ডেটা সংগ্রহ ও সংরক্ষণ করার অনুমতি পেয়েছি? আমরা কি তথ্য খোঁজার জন্য ডেটা প্রক্রিয়া করতে পারি? যদি তাই হয়, বিভিন্ন কলাম হেড সহ অনেক ডেটা ফাইল দিয়ে একটি ডাটাবেস তৈরি করতে হবে। একটি মঞ্চ বা বাজারের জায়গায় ঘটতে পারে এমন কোনও আক্রমণ বা দুর্ঘটনার সতর্কতা নির্ধারণের জন্য, নিচে কিছু ব্যবস্থার পরামর্শ দেওয়া হয়েছে। স্টেজ/লোকেলিটির একটি ডাটা টেবিলের সম্ভাব্য স্কিমা, যেখানে কোনো ইভেন্ট সংগঠিত হবে, তা নিচে উল্লেখ করা হলো:

স্টেজ_টাইপ: খেলার মাঠে, খোলা ভোজসভার ভিতরে, স্থায়ী মঞ্চে হতে পারে

পটভূমি: সিমেন্ট দেয়াল/ফাইবার দেয়াল/কাপড়-কভার/খোলা প্রান্ত

আন্ডার_স্টেজ: খোলা/ঢাকা পাশ/কাপড়-কভার/

ডানদিকে: খোলা/সিমেন্ট দেয়াল/ঢাকা পাশ/কাপড়-কভার/

বামপাশে: খোলা/সিমেন্ট করা দেয়াল/ঢাকা পাশ/কাপড়-কভার/

শীর্ষ: খোলা/ঢাকা পাশ/কাপড়-কভার/শীর্ষের বিষয়বস্তু

স্টেজের_বাইরে: গ্যাস/কেরোসিন-ওভেন/ওয়েল্ডিং মেশিন/ওপেন-রোড

লোড_ক্ষমতা: পরীক্ষিত/ব্যক্তি ক্ষমতা/ওভারলোড-নিয়ন্ত্রণ-কার দ্বারা/

ঝুলন্ত_ফ্যান: পরীক্ষিত/স্থায়ী বা না/অস্থায়ী ঝুলন্ত/

ইত্যাদি।

উপসংহার:

এখানে, কিছু তথ্য সংকলন করা হয়েছে, তবে সীমাবদ্ধ নয়। এগুলি হল কিছু প্রাথমিক তদন্তকারী পয়েন্ট যা নিরাপত্তা কর্মী বা স্বেচ্ছাসেবকদের দ্বারা ইভেন্টের আগে পরীক্ষা করা উচিত। কম্পিউটার সিস্টেমের মধ্যে সংরক্ষণ করার জন্য এই তথ্যগুলিকে ম্যানুয়ালি বা স্বয়ংক্রিয় এবং কাঠামোগত উপায় হিসাবে সংগ্রহ করার পরামর্শ দেওয়া হয়। সচেতনতা আলোচনার স্তর থেকে শুরু হয় এবং তারপর ধীরে ধীরে স্বয়ংক্রিয় ব্যবস্থায় নিয়ে যায়। অনুষ্ঠানের আয়োজক এবং অংশগ্রহণকারীদের তাদের সিকিউরিটিজ সম্পর্কে সচেতন হওয়া উচিত; যদি মানুষ সম্ভাব্য বিপদ সম্পর্কে সচেতন হয়, তবেই ক্ষতির পরিমাণ কমিয়ে আনা সম্ভব।

শেষ